Docket No.: 60188-790 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Ikuko FUJINAWA, et al.	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: March 3, 2004	:	Examiner:

For: DATA PROCESSING DEVICE AND DATA PROCESSING METHOD

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. JP 2003-055626, filed on March 3, 2003.

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:gav
Facsimile: (202) 756-8087
Date: March 3, 2004

60188-790
IKUKO FUJINAWA et al.
March 3, 2004

McDermott, Will & Emery

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月　３日

出願番号
Application Number: 特願２００３－０５５６２６

[ST. 10/C]: [ＪＰ２００３－０５５６２６]

出願人
Applicant(s): 松下電器産業株式会社

２００３年　９月　８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０７３４０８

【書類名】　特許願
【整理番号】　5037720199
【提出日】　平成15年 3月 3日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/14　320
G09C 1/00　310
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　藤縄　幾子
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　樋口　淑夫
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100077931
【弁理士】
【氏名又は名称】　前田　弘
【選任した代理人】
【識別番号】　100094134
【弁理士】
【氏名又は名称】　小山　廣毅
【選任した代理人】
【識別番号】　100110939
【弁理士】
【氏名又は名称】　竹内　宏

【選任した代理人】

【識別番号】　100110940

【弁理士】

【氏名又は名称】　嶋田　高久

【選任した代理人】

【識別番号】　100113262

【弁理士】

【氏名又は名称】　竹内　祐二

【選任した代理人】

【識別番号】　100115059

【弁理士】

【氏名又は名称】　今江　克実

【選任した代理人】

【識別番号】　100115691

【弁理士】

【氏名又は名称】　藤田　篤史

【選任した代理人】

【識別番号】　100117581

【弁理士】

【氏名又は名称】　二宮　克也

【選任した代理人】

【識別番号】　100117710

【弁理士】

【氏名又は名称】　原田　智雄

【選任した代理人】

【識別番号】　100121500

【弁理士】

【氏名又は名称】　後藤　高志

【選任した代理人】

【識別番号】　100121728

【弁理士】

【氏名又は名称】　井関　勝守

【手数料の表示】

【予納台帳番号】　014409

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0217869

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置、および情報処理方法

【特許請求の範囲】

【請求項１】

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ他の鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、

上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理装置であって、

上記暗号化データ、および上記暗号化鍵データの読み込みを制御する読み込み制御部と、

上記読み込み制御部の制御によって読み込まれた暗号化データ、および暗号化鍵データを復号化する復号化部と、

上記復号化部によって上記暗号化鍵データから復号化された鍵データを保持する鍵データ保持部とを備え、

上記復号化部は、上記鍵データ保持部に保持された鍵データに基づいて、上記暗号化データおよび暗号化鍵データを復号化するように構成されていることを特徴とする情報処理装置。

【請求項２】

請求項１の情報処理装置であって、

上記読み込み制御部は、

全ての上記分割データがそれぞれ暗号化されて上記記憶媒体に記憶された各暗号化データと、上記暗号化データをそれぞれ復号化する鍵データが暗号化されて上記記憶媒体に記憶された各暗号化鍵データとを、所定の一意に定まった順序で順次読み込むように構成され、

上記復号化部は、上記鍵データ保持部に保持された鍵データに基づいて、上記記憶媒体から読み込まれた第１の暗号化データおよび第１の暗号化鍵データを復

号化して、第１の分割データおよび第１の鍵データを出力するとともに、
復号化されて上記鍵データ保持部に保持された上記第１の鍵データに基づいて、
上記第１の暗号化データおよび第１の暗号化鍵データに後続して読み込まれた、
第２の暗号化データおよび第２の暗号化鍵データを復号化するように構成されていることを特徴とする情報処理装置。

【請求項３】

請求項１の情報処理装置であって、

上記読み込み制御部は、

上記複数の分割データのうち、一部の分割データが暗号化されて上記記憶媒体に記憶された暗号化データ、

他の分割データが暗号化されることなく上記記憶媒体に記憶された非暗号化データ、および

上記各暗号化データおよび非暗号化データにそれぞれ対応して上記記憶媒体に記憶された暗号化鍵データを、

所定の一意に定まった順序で順次読み込むように構成されるとともに、

上記復号化部は、

上記記憶媒体から第１の暗号化鍵データと第１の暗号化データとが読み込まれた場合には、

これらを上記鍵データ保持部に保持された鍵データに基づき復号化して、第１の分割データおよび第１の鍵データを出力する一方、

上記記憶媒体から第１の暗号化鍵データと第１の非暗号化データとが読み込まれた場合には、

上記第１の暗号化鍵データを上記鍵データ保持部に保持された鍵データに基づき復号化して、第１の鍵データを出力し、

上記第１の暗号化鍵データと第１の暗号化データと、または上記第１の暗号化鍵データと第１の非暗号化データとに後続して読み込まれた、第２の暗号化鍵データ、または第２の暗号化鍵データと第２の暗号化データとを、上記第１の鍵データに基づいて復号化するように構成されていることを特徴とする情報処理装置。

【請求項４】

請求項１の情報処理装置であって、

上記読み込み制御部は、

上記複数の分割データのうち、一部の分割データが暗号化されて上記記憶媒体に記憶された暗号化データ、

他の分割データが暗号化されることなく上記記憶媒体に記憶された非暗号化データ、および

上記各暗号化データに対応して上記記憶媒体に記憶された暗号化鍵データを、

所定の一意に定まった順序で順次読み込むように構成されるとともに、

上記復号化部は、

上記記憶媒体から第１の暗号化鍵データおよび第１の暗号化データが読み込まれた場合には、

これらを上記鍵データ保持部に保持された鍵データに基づき復号化して、第１の分割データおよび第１の鍵データを出力するとともに、

上記第１の暗号化鍵データおよび第１の暗号化データ以降に読み込まれた、第２の暗号化鍵データおよび第２の暗号化データを、上記第１の鍵データに基づいて復号化するように構成されていることを特徴とする情報処理装置。

【請求項５】

請求項１の情報処理装置であって、

上記読み込み制御部は、上記記憶媒体に記憶された第１の暗号化データに後続して、上記第１の暗号化データに対応してあらかじめ定まった１つ以上の第２の暗号化データから成る後続候補群のうちの何れかの第２の暗号化データを読み込むとともに、

上記第１の暗号化データに対応して、それぞれ上記後続候補群の各第２の暗号化データを復号化するための鍵データが暗号化された１つ以上の暗号化鍵データを含む暗号化鍵データ群を読み込むように構成され、

上記鍵データ保持部は、上記記憶媒体から読み込まれた上記暗号化鍵データ群の各暗号化鍵データから復号化された１つ以上の鍵データをを保持し、

上記復号化部は、鍵データ保持部に保持された上記１つ以上の鍵データのうち、上記第１の暗号化データに後続して実際に読み込まれた第２の暗号化データに

対応する鍵データに基づいて、上記第２の暗号化データ、およびその第２の暗号化データに対応して読み込まれた暗号化鍵データ群の各暗号化鍵データを復号化するように構成されていることを特徴とする情報処理装置。

【請求項６】

請求項２から請求項５のうちの何れか１項の情報処理装置であって、

上記記憶媒体に記憶されるべきデータは、上記情報処理装置に実行させる命令を含み、上記暗号化データおよび非暗号化データの読み込み順序が、上記命令のうちの分岐命令によって決定されることを特徴とする情報処理装置。

【請求項７】

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ共通の共通鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、

上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理装置であって、

上記暗号化データ、および上記暗号化鍵データの読み込みを制御する読み込み制御部と、

上記読み込み制御部の制御によって読み込まれた暗号化データ、および暗号化鍵データを復号化する復号化部と、

上記復号化部によって上記暗号化鍵データから復号化された鍵データ、および上記共通鍵データを保持する鍵データ保持部とを備え、

上記復号化部は、上記鍵データ保持部に保持された上記鍵データまたは上記共通鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復号化するように構成されていることを特徴とする情報処理装置。

【請求項８】

請求項７の情報処理装置であって、

上記鍵データ保持部は、上記暗号化鍵データから復号化された鍵データを保持する第１の鍵データ保持部と、上記共通鍵データを保持する第２の鍵データ保持

部とを備え、

上記復号化部は、上記第１の鍵データ保持部に保持された鍵データに基づいて上記暗号化データを復号化する第１の復号化部と、上記第２の鍵データ保持部に保持された共通鍵データに基づいて上記暗号化鍵データを復号化する第２の復号化部とを備えたことを特徴とする情報処理装置。

【請求項９】

請求項８の情報処理装置であって、

さらに、上記第２の復号化部によって上記暗号化鍵データの復号化が行われる間に、上記記憶媒体に対して、次に読み込むべきデータとは異なる領域に記憶されているデータを読み込むのと同じ信号を出力する擬似読み込み信号出力部を備えたことを特徴とする情報処理装置。

【請求項１０】

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ他の鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、

上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理方法であって、

上記暗号化データ、および上記暗号化鍵データを読み込む読み込みステップと、

上記読み込みステップによって読み込まれた暗号化データ、および暗号化鍵データを復号化し、上記暗号化鍵データから復号化された鍵データを鍵データ保持部に保持させる復号化ステップとを有し、

上記復号化ステップは、上記鍵データ保持部に保持された上記鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復号化することを特徴とする情報処理方法。

【請求項１１】

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも

一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ共通の共通鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、

上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理方法であって、

上記暗号化データ、および上記暗号化鍵データを読み込む読み込みステップと、

上記読み込みステップによって読み込まれた暗号化データ、および暗号化鍵データを復号化し、上記暗号化鍵データから復号化された鍵データを鍵データ保持部に保持させる復号化ステップとを有し、

上記復号化ステップは、上記鍵データ保持部に保持された上記鍵データまたは上記共通鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復号化することを特徴とする情報処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、メモリや、ＩＣカード、ハードディスクなどの記憶媒体に記憶されたデータが容易に第三者に漏洩することの防止に関する技術に属する。

【０００２】

【従来の技術】

従来より、メモリなどの記憶媒体に記憶されたデータ、特にＣＰＵに実行させる一連の命令コードから成るプログラムとしてのデータが第三者に漏洩するのを防ぐために、データの暗号化を用いる技術が知られている。具体的には、例えば特許文献１に記載されているように、あらかじめ、記憶媒体に記憶されたデータを読み出す装置に固定的に設定され、または記憶データごとに任意に設定された暗号鍵（復号鍵）を用い、記憶媒体から読み出された暗号化されたデータを順次復号化して、装置内のＣＰＵに入力するように構成したデータ保護装置が知られている。

【０００３】

【特許文献１】

特開平７－１２９４７３号公報

【０００４】

【発明が解決しようとする課題】

しかしながら、上記のような従来の装置では、暗号化されたデータを復号化する暗号鍵として単一の暗号鍵が用いられているために、復号化方法（アルゴリズム）とともに、１つの暗号鍵が漏洩してしまうと、記憶媒体に記憶されている全てのデータが漏洩してしまうという問題が生じる。

【０００５】

なお、上記のような全てのデータの漏洩を防止するためには、記憶媒体に記憶させるデータを複数のブロックに分割し、各ブロックごとに別個の暗号鍵を用いて暗号化、復号化を行うようにすることも考えられるが、そのためには、複数の暗号鍵を各ブロックと対応づけて扱う必要があり、暗号化、復号化処理や暗号鍵の管理の複雑化を招くことになる。

【０００６】

上記の問題に鑑み、本発明は、暗号鍵の管理の複雑化などを招くことなく、記憶媒体に記憶されたデータが容易に第三者に漏洩するのを防止可能にすることを課題とする。

【０００７】

【課題を解決するための手段】

前記の課題を解決するために、請求項１の発明が講じた解決手段は、

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ他の鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、

上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理装置であって、

上記暗号化データ、および上記暗号化鍵データの読み込みを制御する読み込み制御部と、

上記読み込み制御部の制御によって読み込まれた暗号化データ、および暗号化鍵データを復号化する復号化部と、

上記復号化部によって上記暗号化鍵データから復号化された鍵データを保持する鍵データ保持部とを備え、

上記復号化部は、上記鍵データ保持部に保持された鍵データに基づいて、上記暗号化データおよび暗号化鍵データを復号化するように構成されていることを特徴とする。

【０００８】

これによると、各分割データが、それぞれ異なる鍵データによって復号化されるように暗号化されているので、万一、一部の鍵データが漏洩したとしても、記憶媒体の記憶内容全体を容易に知られてしまうことがない。しかも、各鍵データは、それぞれ他の鍵データによって復号化されるように暗号化されて記憶媒体に記憶されているので、複数の鍵データを管理する必要がなく、管理の複雑化を招くことがない。

【０００９】

また、請求項２の発明は、

請求項１の情報処理装置であって、

上記読み込み制御部は、

全ての上記分割データがそれぞれ暗号化されて上記記憶媒体に記憶された各暗号化データと、上記暗号化データをそれぞれ復号化する鍵データが暗号化されて上記記憶媒体に記憶された各暗号化鍵データとを、所定の一意に定まった順序で順次読み込むように構成され、

上記復号化部は、上記鍵データ保持部に保持された鍵データに基づいて、上記記憶媒体から読み込まれた第１の暗号化データおよび第１の暗号化鍵データを復号化して、第１の分割データおよび第１の鍵データを出力するとともに、

復号化されて上記鍵データ保持部に保持された上記第１の鍵データに基づいて、上記第１の暗号化データおよび第１の暗号化鍵データに後続して読み込まれた、

第２の暗号化データおよび第２の暗号化鍵データを復号化するように構成されていることを特徴とする。

【００１０】

これによると、記憶媒体に記憶された各暗号化データと各暗号化鍵データとが所定の順序で読み込まれることにより、各暗号化データ、および次の暗号化データを復号化するための暗号化鍵データが順次読み込まれて復号化されるので、暗号化前の元のデータを容易に得ることができる。

【００１１】

また、請求項３の発明は、

請求項１の情報処理装置であって、

上記読み込み制御部は、

上記複数の分割データのうち、一部の分割データが暗号化されて上記記憶媒体に記憶された暗号化データ、

他の分割データが暗号化されることなく上記記憶媒体に記憶された非暗号化データ、および

上記各暗号化データおよび非暗号化データにそれぞれ対応して上記記憶媒体に記憶された暗号化鍵データを、

所定の一意に定まった順序で順次読み込むように構成されるとともに、

上記復号化部は、

上記記憶媒体から第１の暗号化鍵データと第１の暗号化データとが読み込まれた場合には、

これらを上記鍵データ保持部に保持された鍵データに基づき復号化して、第１の分割データおよび第１の鍵データを出力する一方、

上記記憶媒体から第１の暗号化鍵データと第１の非暗号化データとが読み込まれた場合には、

上記第１の暗号化鍵データを上記鍵データ保持部に保持された鍵データに基づき復号化して、第１の鍵データを出力し、

上記第１の暗号化鍵データと第１の暗号化データと、または上記第１の暗号化鍵データと第１の非暗号化データとに後続して読み込まれた、第２の暗号化鍵デー

タ、または第２の暗号化鍵データと第２の暗号化データとを、上記第１の鍵データに基づいて復号化するように構成されていることを特徴とする。

【００１２】

これによると、混在して記憶された暗号化データと非暗号化データとが読み込まれるようにすることにより、復号化動作を最小限に抑えて、読み込み速度の低下を防止することが容易にできる。

【００１３】

また、請求項４の発明は、

請求項１の情報処理装置であって、

上記読み込み制御部は、

上記複数の分割データのうち、一部の分割データが暗号化されて上記記憶媒体に記憶された暗号化データ、

他の分割データが暗号化されることなく上記記憶媒体に記憶された非暗号化データ、および

上記各暗号化データに対応して上記記憶媒体に記憶された暗号化鍵データを、

所定の一意に定まった順序で順次読み込むように構成されるとともに、

上記復号化部は、

上記記憶媒体から第１の暗号化鍵データおよび第１の暗号化データが読み込まれた場合には、

これらを上記鍵データ保持部に保持された鍵データに基づき復号化して、第１の分割データおよび第１の鍵データを出力するとともに、

上記第１の暗号化鍵データおよび第１の暗号化データ以降に読み込まれた、第２の暗号化鍵データおよび第２の暗号化データを、上記第１の鍵データに基づいて復号化するように構成されていることを特徴とする。

【００１４】

これによると、各鍵データは、次に読み込まれる暗号化データおよびこれに対応する暗号化鍵データの復号化に用いられ、非暗号化データに対応する暗号化鍵データを復号化することなどが必要ないので、より、読み込み速度の低下を防止したり、記憶データ量の増加を小さく抑えたりすることができる。

【００１５】

また、請求項５の発明は、

請求項１の情報処理装置であって、

上記読み込み制御部は、上記記憶媒体に記憶された第１の暗号化データに後続して、上記第１の暗号化データに対応してあらかじめ定まった１つ以上の第２の暗号化データから成る後続候補群のうちの何れかの第２の暗号化データを読み込むとともに、

上記第１の暗号化データに対応して、それぞれ上記後続候補群の各第２の暗号化データを復号化するための鍵データが暗号化された１つ以上の暗号化鍵データを含む暗号化鍵データ群を読み込むように構成され、

上記鍵データ保持部は、上記記憶媒体から読み込まれた上記暗号化鍵データ群の各暗号化鍵データから復号化された１つ以上の鍵データをを保持し、

上記復号化部は、鍵データ保持部に保持された上記１つ以上の鍵データのうち、上記第１の暗号化データに後続して実際に読み込まれた第２の暗号化データに対応する鍵データに基づいて、上記第２の暗号化データ、およびその第２の暗号化データに対応して読み込まれた暗号化鍵データ群の各暗号化鍵データを復号化するように構成されていることを特徴とする。

【００１６】

また、請求項６の発明は、

請求項２から請求項５のうちの何れか１項の情報処理装置であって、

上記記憶媒体に記憶されるべきデータは、上記情報処理装置に実行させる命令を含み、上記暗号化データおよび非暗号化データの読み込み順序が、上記命令のうちの分岐命令によって決定されることを特徴とする。

【００１７】

これらによると、分岐命令の実行などによって、各暗号化データの読み込み順序が一意に定まらないような場合でも、各暗号化データの次に読み込まれる可能性のある各暗号化データを復号化するための鍵データが復号化されて保持されるので、何れの暗号化データが読み込まれる場合でも適切に復号化されるようにすることができる。それゆえ、柔軟な順序で暗号化データを読み込ませることがで

き、したがって、記憶媒体に記憶させるデータの作成や分割を柔軟に行うことなどができる。

【００１８】

また、請求項７の発明は、

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および

上記鍵データが、それぞれ共通の共通鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、

上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理装置であって、

上記暗号化データ、および上記暗号化鍵データの読み込みを制御する読み込み制御部と、

上記読み込み制御部の制御によって読み込まれた暗号化データ、および暗号化鍵データを復号化する復号化部と、

上記復号化部によって上記暗号化鍵データから復号化された鍵データ、および上記共通鍵データを保持する鍵データ保持部とを備え、

上記復号化部は、上記鍵データ保持部に保持された上記鍵データまたは上記共通鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復号化するように構成されていることを特徴とする。

【００１９】

これによると、各暗号化鍵データは、共通鍵データによって復号化されるので、暗号化データや暗号化鍵データの読み込み順序には依存せずに復号化することができる。それゆえ、やはり、柔軟な順序で暗号化データを読み込ませることなどができる。

【００２０】

また、請求項８の発明は、

請求項７の情報処理装置であって、

上記鍵データ保持部は、上記暗号化鍵データから復号化された鍵データを保持

する第１の鍵データ保持部と、上記共通鍵データを保持する第２の鍵データ保持部とを備え、

上記復号化部は、上記第１の鍵データ保持部に保持された鍵データに基づいて上記暗号化データを復号化する第１の復号化部と、上記第２の鍵データ保持部に保持された共通鍵データに基づいて上記暗号化鍵データを復号化する第２の復号化部とを備えたことを特徴とする。

【００２１】

これによると、暗号化データまたは暗号化鍵データを復号化するための復号化部や鍵データ保持部が別個に設けられることによって、暗号化データと暗号化鍵データとを互いに異なるアルゴリズムによって復号化することなどができるので、暗号化強度と読み込み速度とのバランスをとることなどが容易にできる。

【００２２】

また、請求項９の発明は、

請求項８の情報処理装置であって、

さらに、上記第２の復号化部によって上記暗号化鍵データの復号化が行われる間に、上記記憶媒体に対して、次に読み込むべきデータとは異なる領域に記憶されているデータを読み込むのと同じ信号を出力する擬似読み込み信号出力部を備えたことを特徴とする。

【００２３】

これによると、暗号化鍵データの復号化が行われる際に、その復号化によって得られた鍵データにより復号化される次のデータが読み出されるまでにタイムラグがある場合などでも、例えば乱数に基づく疑似的なアドレス信号などが出力されることによって、情報処理装置の外部からは暗号化鍵データの復号化が行われていることを察知することなどが困難になる。それゆえ、悪意の者が解析によって記憶内容を取得することなどを一層困難にすることができる。

【００２４】

また、請求項１０の発明は、

記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号

化された暗号化データ、および
上記鍵データが、それぞれ他の鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、
上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理方法であって、
上記暗号化データ、および上記暗号化鍵データを読み込む読み込みステップと、
上記読み込みステップによって読み込まれた暗号化データ、および暗号化鍵データを復号化し、上記暗号化鍵データから復号化された鍵データを鍵データ保持部に保持させる復号化ステップとを有し、
上記復号化ステップは、上記鍵データ保持部に保持された上記鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復号化することを特徴とする。

【００２５】

また、請求項１１の発明は、
記憶されるべきデータが複数の分割データに分割され、そのうちの少なくとも一部の分割データが、それぞれ異なる鍵データによって復号化されるように暗号化された暗号化データ、および
上記鍵データが、それぞれ共通の共通鍵データによって復号化されるように暗号化された暗号化鍵データが記憶された記憶媒体から、
上記暗号化データおよび上記暗号化鍵データを読み込んで復号化する情報処理方法であって、
上記暗号化データ、および上記暗号化鍵データを読み込む読み込みステップと、
上記読み込みステップによって読み込まれた暗号化データ、および暗号化鍵データを復号化し、上記暗号化鍵データから復号化された鍵データを鍵データ保持部に保持させる復号化ステップとを有し、
上記復号化ステップは、上記鍵データ保持部に保持された上記鍵データまたは上記共通鍵データに基づいて、上記暗号化データおよび上記暗号化鍵データを復

号化することを特徴とする。

【００２６】

これらによっても、前記請求項１や請求項７について説明したように、やはり、鍵データの管理の複雑化を招いたりすることなく、記憶内容の秘匿性を高めることが容易にできる。

【００２７】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照して説明する。

【００２８】

（実施の形態１）

（装置の構成）

図１は本発明の実施の形態１に係る情報処理装置の例としてのマイクロコンピュータ１００の要部の構成、および上記マイクロコンピュータ１００に接続された記憶媒体としてのメモリ１２０を示すブロック図である。

【００２９】

上記メモリ１２０は、例えばＲＯＭやＲＡＭによって構成され、マイクロコンピュータ１００に実行させる命令の命令コードから成るプログラムが暗号化されたデータを記憶し、アドレスバスによって示されるアドレスに応じたデータをデータバスに出力するようになっている。このメモリ１２０には、例えば図２に示すように、一連の命令コードから成るプログラム（データ）が５つのデータブロック２０１～２０５として記憶されているが、その記憶形式については、後に詳述する。

【００３０】

マイクロコンピュータ１００には、ＣＰＵ１０１（読み込み制御部）と、復号化部１０２と、鍵データ保持部１０３と、選択部１０４と、選択指示保持部１０５と、復号化情報管理部１０６とが設けられている。

【００３１】

上記ＣＰＵ１０１は、命令コードの実行処理を行うものである。このＣＰＵ１０１には、復号化制御部１０１ａが設けられている。上記復号化制御部１０１ａ

は、メモリ１２０に記憶された各データブロック２０１～２０５が読み込まれる際に、各データブロック２０１～２０５に含まれる復号化情報２１１～２１５を読み込んで、鍵データ（復号鍵）等を復号化情報管理部１０６に出力するなどの制御を行うようになっている。

【００３２】

復号化部１０２は、鍵データ保持部１０３に設定された鍵データを用いて、メモリ１２０から出力された暗号化データを復号化するものである。

【００３３】

選択部１０４は、選択指示保持部１０５に設定された選択指示に基づいて、上記復号化部１０２から復号化されて出力されるデータ、またはメモリ１２０から直接出力された（平文の）データの何れか一方を選択し、内部バスを介してＣＰＵ１０１に入力するようになっている。ただし、ＣＰＵ１０１から例えばＨ（High）レベルの復号化情報読み込み信号が入力される場合には、上記選択指示保持部１０５に設定された選択指示に係らず、復号化部１０２の出力を選択するようになっている。

【００３４】

復号化情報管理部１０６は、上記鍵データ保持部１０３に設定される鍵データ、および選択指示保持部１０５に設定される選択指示を管理するようになっている。より詳しくは、ＣＰＵ１０１から（図示しない出力タイミング信号と伴に）出力される鍵データを鍵データ一時保持部１０６ａに一旦保持するとともに、この保持された鍵データを、メモリ１２０から各データブロック２０１～２０５の復号化情報２１１～２１５が読み込まれる前に、鍵データ保持部１０３に設定するようになっている。また、ＣＰＵ１０１から（図示しない出力タイミング信号と伴に）出力される選択部１０４への選択指示を選択指示一時保持部１０６ｂに一旦保持するとともに、この保持された選択指示を、各データブロック２０１～２０５に含まれる実行ブロック２２１～２２５が読み込まれる前に、選択部１０４に設定するようになっている。（また、上記設定が完了すると、ＣＰＵ１０１に設定終了信号を出力して、次のアドレスの出力などの動作をさせ得るようになっている。なお、上記設定が例えば１クロックサイクル内に行われる場合などに

は、ＣＰＵ１０１に次の動作を適切なタイミングで行わせることが容易にできるので、必ずしも上記のような設定終了信号を出力するようにしなくてもよい。）上記鍵データ一時保持部１０６ａ、および選択指示一時保持部１０６ｂには、上記のようにＣＰＵ１０１から出力された鍵データ等が一旦保持される他、さらに、最初のデータブロックが読み込まれる際にマイクロコンピュータ１００の外部から入力された鍵データ等が保持されるようになっている。

【００３５】

ここで、メモリ１２０に記憶されるデータの暗号化方式としては種々のものを適用することができ、特に限定されないが、例えば、ＤＥＳ暗号方式のように１つの暗号鍵によって暗号化および復号化が行われる、可逆変換が可能な共通鍵暗号方式や、暗号鍵を初期値として、順次入力されるデータの排他的論理和演算を行う方式などを用いることができる。

【００３６】

なお、マイクロコンピュータ１００には、通常、上記の他にも、一時的なデータ等を保持するＲＡＭや、外部の装置との間で入出力を行うインタフェイス、また、メモリ１２０がデータの書き込みも可能な記憶媒体である場合には書き込み制御部などを備えているが、本発明の主眼ではないのでここでは省略する。

【００３７】

また、マイクロコンピュータ１００は、例えば１チップのＬＳＩで構成される場合には、上記各部間の信号を解析することなどが一層困難になるので、より秘匿性を高めることができるが、これに限るものではない。

【００３８】

（メモリ１２０に記憶されるデータの形式）

メモリ１２０には、図２に示すように、それぞれ復号化情報２１１～２１５と実行ブロック２２１～２２５とを含む複数（同図の例では５つ）のデータブロック２０１～２０５が記憶されている。これらのデータブロック２０１～２０５のＣＰＵ１０１への読み込みは、データブロック２０１～２０５に含まれるポインタ等に基づいて、あらかじめ定められた一定の順序で行われるようになっている。（ここでは説明の簡単化のために、データブロック２０１～２０５の順で読み

込まれるとして説明する。）

上記実行ブロック２２１～２２５は、例えば図３に示すように、一連の命令コードから成るプログラム（データ）が５つの実行単位に分割された命令コード列２２１ａ～２２５ａに実行終了コード２３０が付加されて構成されている。上記実行終了コード２３０としては、具体的には、例えば分岐先のデータブロックを特定して分岐する専用の命令を用いたり、通常の分岐命令と、分岐先が他のデータブロックであることを示すフラグをセットする命令とを組み合わせて用いたり、通常の分岐命令を用いて、分岐先のアドレスなどによってＣＰＵ１０１が他のデータブロックへの分岐であることを検出し得るようにしたりしてもよい。さらに、通常の分岐命令で他のデータブロックのアドレスに分岐した後に、分岐先のデータブロックまたは実行ブロックの先頭に、データブロックが変わったことを示す（復号化情報の読み込みなどの処理をさせる）命令を設けるなどしてもよい。なお、分岐先のデータブロックをアドレスによって特定する場合、そのアドレスとしては、復号化情報の先頭のアドレスを指定するようにしてもよいし、実行ブロックの先頭のアドレス等を指定して、復号化情報のデータ長などから復号化情報の先頭のアドレスを求め得るようにしてもよい。

【００３９】

また、復号化情報２１１～２１５には、それぞれ、鍵データ２１１ａ～２１５ａと暗号化有無情報２１１ｂ～２１５ｂとが含まれている。（なお、復号化情報２１１～２１５は、データブロック２０１～２０５の先頭に限らず、実行ブロック２２１～２２５の内部や末尾などに配置されるようにしてもよい。また、データブロック２０５の次に読み込まれるデータブロックがない場合、すなわち、データブロック２０５内の命令が繰り返し実行されて、他のデータブロックに移行しない場合には、鍵データ２１５ａおよび暗号化有無情報２１５ｂの内容は不定でよく、さらに、これらの情報を省略することもできる。）

上記復号化情報２１１～２１５は全て暗号化されている一方、実行ブロック２２１～２２５は必要に応じて（例えば実行ブロック２２２・２２４が）暗号化されている。上記暗号化されたデータを復号化するための鍵データは、それぞれのデータブロック２０１～２０５ごとに異なり、各データブロック２０２～２０５

を復号化する鍵データは、それぞれのデータブロック２０２～２０５の直前に読み込まれるデータブロック２０１～２０４の復号化情報２１１～２１４に含まれている。すなわち、例えばデータブロック２０１の復号化情報２１１に含まれる鍵データ２１１ａによって、次に読み込まれるデータブロック２０２の復号化情報２１２および実行ブロック２２２を復号化することができるようになっている。なお、最初に実行されるデータブロック２０１（の少なくとも復号化情報２１１）を復号化するための鍵データ２１０ａは、メモリ１２０中には記憶されておらず、実行時にマイクロコンピュータ１００の外部から与えられるようになっている。（ここで、上記鍵データは、必ずしも全てが互いに異ならなくてもよい。すなわち、例えば有限個の鍵データから選択された鍵データが用いられるなどして、一部のデータブロックに同じ鍵データが用いられることがあってもよい。）

また、復号化情報２１１～２１４に含まれる暗号化有無情報２１１ｂ～２１４ｂは、次のデータブロック２０２～２０５の実行ブロック２２２～２２５が暗号化されているかどうかを示し、例えば、各データブロックの次に実行されるデータブロックの実行ブロックが暗号化されている場合には、値０ｘ００１０（「０ｘ」は続く数値が１６進数表記であることを示す。）が設定される一方、暗号化されていない場合には、値０ｘ０００１が設定されている。より具体的には、前記のようにデータブロック２０２・２０４の実行ブロック２２２・２２４が暗号化されている場合には、これらの直前に読み込まれるデータブロック２０１・２０３の暗号化有無情報２１１ｂ・２１３ｂには０ｘ００１０が設定され、その他のデータブロック２０２・２０４の暗号化有無情報２１２ｂ・２１４ｂには０ｘ０００１が設定されている。

【００４０】

上記のようなデータを生成してメモリ１２０に保存する手順は特に限定されないが、例えば図４に示すようにして行うことができる。まず、一連の命令コードから成るプログラムを（例えば所定のデータ長ごと、またはその前後の分岐命令を区切りとして）５つの命令コード列２２１ａ～２２５ａに分割し（Ｓ１０１）、各データブロック２０１～２０５の復号化情報２１１～２１５等および実行ブロック２２２・２２４をそれぞれ暗号化するための鍵データ２１０ａ～２１５ａ

を乱数を用いるなどして自動的に、または人為的に定め（Ｓ１０２）、上記鍵データ２１１ａ～２１５ａと暗号化有無情報２１１ｂ～２１５ｂとを連結して復号化情報２１１～２１５を生成し（Ｓ１０３）、上記分割された命令コード列２２１ａ～２２５ａに実行終了コード２３０を付加して実行ブロック２２１～２２５を生成するとともに、これらの実行ブロック２２１～２２５と復号化情報２１１～２１５とをそれぞれ連結してデータブロック２０１～２０５を構成し（Ｓ１０４）、全ての復号化情報２１１～２１５を鍵データ２１０ａ～２１４ａで暗号化し、実行ブロック２２２・２２４を鍵データ２１１ａ・２１３ａで暗号化して（Ｓ１０５）、メモリ１２０に格納する（Ｓ１０６）。

【００４１】

（メモリ１２０に記憶されたデータの読み込みと実行動作）

上記のようにメモリ１２０に記憶されたプログラムがマイクロコンピュータ１００に読み込まれて実行される場合の動作について、図５に基づいて説明する。

【００４２】

（Ｓ２０１）　マイクロコンピュータ１００の外部から、最初に読み込まれるデータブロック２０１についての鍵データ２１０ａ、および選択指示が入力されると、これらを復号化情報管理部１０６の鍵データ一時保持部１０６ａ、および選択指示一時保持部１０６ｂが保持する。

【００４３】

（Ｓ２０２）　復号化制御部１０１ａの制御によって、ＣＰＵ１０１が復号化情報管理部１０６および選択部１０４にＨレベルの復号化情報読み込み信号を出力する。これに応じて、復号化情報管理部１０６の鍵データ一時保持部１０６ａ、および選択指示一時保持部１０６ｂに保持されている、鍵データおよび選択指示が、それぞれ鍵データ保持部１０３または選択指示保持部１０５に設定される。また、選択部１０４は、上記選択指示保持部１０５に設定された選択指示に係らず、復号化部１０２からの出力を選択して１０１に出力するように切り替わる。

【００４４】

（Ｓ２０３）　復号化制御部１０１ａの制御によって、ＣＰＵ１０１がメモリ

１２０に復号化情報を読み込むためのアドレス（および図示しない読み出し制御信号）を出力する。これに応じて、メモリ１２０は復号化情報を出力する。

【００４５】

（Ｓ２０４）　復号化部１０２は、メモリ１２０から出力された復号化情報を鍵データ保持部１０３に設定された鍵データに基づいて復号化し、選択部１０４は上記復号化部１０２の出力を選択してＣＰＵ１０１に入力する。

【００４６】

（Ｓ２０５）　復号化制御部１０１ａは、上記復号化情報に含まれる鍵データを抽出して復号化情報管理部１０６に出力し、鍵データ一時保持部１０６ａに一旦保持させる。また、復号化情報に含まれる暗号化有無情報に基づいて、すなわち、次のデータブロックの実行ブロックが暗号化されているかどうかに応じて、復号化情報管理部１０６の選択指示一時保持部１０６ｂに、復号化部１０２またはメモリ１２０の何れからの出力を選択部１０４に選択させるかを示す選択指示を一旦保持させる。（これらの鍵データおよび選択指示は、次のデータブロックを読み込むために再度（Ｓ２０２）が実行される際に鍵データ保持部１０３および選択指示保持部１０５に設定される。）

（Ｓ２０６）　マイクロコンピュータ１００から出力される復号化情報読み込み信号がＬ（Low）レベルになると、選択部１０４は、選択指示保持部１０５に設定されている選択指示に基づいて、復号化部１０２の出力またはメモリ１２０の出力を選択的にＣＰＵ１０１に入力するように切り替わる。

【００４７】

（Ｓ２０７）　ＣＰＵ１０１が実行ブロックの各命令コードに応じたアドレスを出力し、メモリ１２０から出力された命令コードは、選択部１０４を介し、暗号化の有無に応じて、すなわち暗号化されている場合には復号化部１０２により復号化された後、または平文である場合にはそのまま、ＣＰＵ１０１に入力される。

【００４８】

（Ｓ２０８）　メモリ１２０から出力されたのが実行終了コード２３０であれば、（Ｓ２０２）に戻って次のデータブロックについて同じ処理が繰り返される

。（すなわち、鍵データ一時保持部１０６ａおよび選択指示一時保持部１０６ｂに一旦保持された鍵データおよび選択指示が鍵データ保持部１０３および選択指示保持部１０５に設定されて、これらに基づいて次のデータブロックの読み込み等が行われる。）

（Ｓ２０９）　一方、メモリ１２０から出力されたのが実行終了コード２３０でなければ、ＣＰＵ１０１は読み込まれた命令コードの命令を実行し、実行終了コード２３０が読み込まれるまで、（Ｓ２０７）～（Ｓ２０９）を繰り返す。

【００４９】

上記のような動作が行われることにより、マイクロコンピュータ１００に外部から与える必要のある鍵データは、最初に読み込まれるデータブロック２０１についての１つの鍵データだけなので、鍵データの管理の複雑化を招いたりすることがない一方、万一上記１つの鍵データが漏洩したとしても、その鍵データによって復号化できるのは最初のデータブロック２０１だけであり、他のデータブロックを復号化するための鍵データはそれぞれさらに他の鍵データによって暗号化されているので、メモリ１２０に記憶されている全てのデータが容易に知られてしまうことはない。すなわち、理論的には、１つの鍵データが知られてしまうと、それを基に復号化情報の復号化、次の鍵データの抽出を繰り返すことによって全てのデータを得ることは不可能ではないが、そのためには、暗号化アルゴリズムも知る必要があるとともに、実行ブロック２２１～２２５を解析するなどして、各データブロック２０１～２０５の区切りや読み込み順序等を判別する必要があるうえ、復号化情報２１１～２１５のフォーマットやデータブロック２０１～２０５内での位置（各データブロック２０１～２０５の先頭に配置されているとは限らない。）などを認識する必要があるので、メモリ１２０の記憶内容を解読することは相当に困難なものとなる。そして、その困難性が高いほど、解読に要する労力や費用、時間が増大するため、実際上、記憶内容の漏洩を防止することが容易にできる。

【００５０】

上記のように記憶媒体に記憶された内容の秘匿性を高めることができるので、このような情報処理装置を例えばネットワークを介した通信を行う機器に適用す

ることによって、送受されるデータの暗号化処理や通信相手が正しいかどうかを確認する認証処理などを行うプログラム（アルゴリズムやプロトコル）が解読されるのを防止して、通信のセキュリティを確保することなども容易にできる。

【００５１】

なお、前記の例では、実行ブロック２２１～２２５のうちの何れかについてだけ暗号化する例を示したが、これに限らず全て暗号化するようにしてもよい。その場合には、選択部１０４および選択指示保持部１０５や、復号化情報管理部１０６の選択指示一時保持部１０６ｂ等は設けず、常にメモリ１２０の出力が復号化部１０２を介してＣＰＵ１０１に入力されるようにすることができ、また、復号化情報２１１～２１５に暗号化有無情報２１１ｂ～２１５ｂを含めないようにすることもできる。それゆえ、マイクロコンピュータ１００の構成の簡素化等を図ることができる。一方、前記の例のように一部の実行ブロックだけ暗号化する場合、すなわち、例えば規格化された手順の処理を行うプログラム（ルーチン）など、第三者に漏洩しても問題とならないような部分を暗号化しないようにする場合には、復号化に要する処理時間の影響を小さく抑えることが容易にできる。

【００５２】

また、一部の実行ブロックについてだけ暗号化する場合、暗号化された実行ブロックを含むデータブロック（暗号化データブロック）にだけ、鍵データを含めるようにしてもよい。すなわち、暗号化データブロックに、その後に最初に読み込まれる暗号化データブロックの鍵データおよび実行ブロックを復号化する鍵データを含めるようにすれば、暗号化されない実行ブロックを含むデータブロックについては、鍵データを含めないようにでき、復号化部１０２による復号化動作も不要にすることができる。（なお、鍵データを含める必要がない場合でも、乱数を設定するなどして、復号化情報の長さが一定になるようにしたりしてもよい。）

また、各データブロックには、次のデータブロック（または次の暗号化データブロック）の鍵データと実行ブロックを復号化する鍵データを含める例を示したが、そのデータブロック自体に含まれる実行ブロックと、次のデータブロック（または次の暗号化データブロック）に含まれる鍵データとを復号化する鍵データ

を含めるようにしてもよい。すなわち、各データブロックに含まれる鍵データの読み込みが完了するまでは、鍵データ保持部１０３に保持された、以前のデータブロックの実行ブロックを復号化したのと同じ鍵データを用いて復号化し、その復号化が完了して実行ブロックの読み込みが開始される時点で、上記復号化された新たな鍵データが鍵データ保持部１０３に設定されて用いられるようにすればよい。また、このような場合などにおいて、新たな鍵データが復号化された直後に、その新たな鍵データが用いられる場合には、鍵データ一時保持部１０６ａや選択指示一時保持部１０６ｂは必ずしも設けなくてもよい。

【００５３】

（実施の形態２）

上記実施の形態１のマイクロコンピュータは、データブロックの読み込み順序が一定であるような記憶内容を読み込むように構成されているのに対し、例えば条件分岐命令の実行などによって、あるデータブロックの次に読み込まれるデータブロックが必ずしも一定ではないような場合でも記憶内容を適切に読み込ませることができるマイクロコンピュータの例について説明する。すなわち、このマイクロコンピュータでは、データブロック中に含まれた、次に読み込む可能性がある全てのデータブロックについての鍵データを読み込んで保持しておくことにより、柔軟な順序でデータブロックを読み込むことができるようになっている。なお、以下の実施の形態において、前記実施の形態１等と同様の機能を有する構成要素等については同一の符号を付して説明を省略する。

【００５４】

（装置の構成）

図６は本発明の実施の形態２のマイクロコンピュータ３００の要部の構成とメモリ１２０を示すブロック図である。このマイクロコンピュータ３００は、実施の形態１（図１）のマイクロコンピュータ１００と比べて、ＣＰＵ１０１、選択部１０４、および復号化情報管理部１０６に代えて、ＣＰＵ３０１、選択部３０４、および復号化情報管理部３０６を備えている点が異なっている。

【００５５】

ＣＰＵ３０１には、メモリ１２０に記憶されたデータブロックにおける復号化

情報の読み込み動作を制御する復号化制御部３０１ａが設けられている。この復号化制御部３０１ａと実施の形態１の復号化制御部１０１ａとの相違は、後述するようにメモリ１２０に記憶されるデータブロックの形式が実施の形態１とは異なることに対応するものである。

【００５６】

選択部３０４は、選択指示保持部１０５に設定された選択指示に応じてメモリ１２０または復号化部１０２の出力を選択する点は実施の形態１の選択部１０４と同じであるが、上記選択指示に係らず、例えばＣＰＵ３０１から入力されるデータブロック番号・鍵データ数読み込み信号がＨレベルになった場合には、メモリ１２０の出力が直接選択される一方、鍵情報読み込み信号がＨレベルになった場合には、復号化部１０２の出力が選択されるようになっている。

【００５７】

復号化情報管理部３０６は、鍵テーブル３０６ａと制御部３０６ｂとを備えている。上記鍵テーブル３０６ａは、ＣＰＵ３０１から、鍵番号、鍵データ、および選択指示が入力されると、例えば図７に示すように、上記鍵番号と対応させて、鍵データと選択指示とを保持するようになっている。また、制御部３０６ｂは、ＣＰＵ３０１から入力されるデータブロック番号に基づいて、そのデータブロック番号に一致する鍵番号と対応して鍵テーブル３０６ａに保持されている鍵データと選択指示とを出力するようになっている。

【００５８】

（メモリ１２０に記憶されるデータの形式）

また、メモリ１２０には、実施の形態１と同様に複数の（例えば７つの）データブロック４０１～４０７が記憶されているが、各データブロック４０１～４０７は、例えば図８に示すような構造を有している。すなわち、例えば主にデータブロック４０１を代表として説明すると、データブロック４０１には、データブロック番号４２１、鍵データ数４３１、および１つ以上の鍵情報４４１を含む復号化情報４１１と、実行ブロック４５１とが含まれている。各データブロック４０１～４０７の鍵情報４４１～４４７は全て暗号化される一方、実行ブロック４５１～４５７は必要に応じて（例えばデータブロック４０１・４０２の実行ブロ

ック４５１・４５２だけが）暗号化されている。

【００５９】

上記復号化情報４１１のデータブロック番号４２１はデータブロックを特定するもので、データブロック４０１と一意に対応付けて設定されている。

【００６０】

鍵データ数４３１は、復号化情報４１１中に含まれる鍵情報４４１の数（すなわち、後述するようにデータブロック４０１の次に読み込まれる可能性があるデータブロックの数）を示すもので、ＣＰＵ３０１がデータブロック４０１中の全ての鍵情報４４１を読み込むために用いられる。なお、鍵データ数４３１を用いるのに代えて、復号化情報４１１の末尾に、復号化情報４１１の末尾であることを示す終了コードを設けて、鍵情報４４１の読み込み処理を完了させ得るようにしてもよい。

【００６１】

鍵情報４４１は、データブロック４０１の次にＣＰＵ３０１に読み込まれる可能性がある１つ以上のデータブロックに対応して設けられ、それぞれ、鍵番号４４１ａと、鍵データ４４１ｂと、暗号化有無情報４４１ｃとを含んでいる。具体的には、例えばデータブロック４０１の次に、後述するデータブロック分岐命令などによってデータブロック４０２の実行ブロック４５２またはデータブロック４０３の実行ブロック４５３が選択的に実行されるとし、前記のようにデータブロック４０２の実行ブロック４５２は暗号化される一方、データブロック４０３の実行ブロック４５３は暗号化されないとすると、復号化情報４１１には次のような２つの鍵情報４４１が設けられる。

【００６２】

すなわち、一方の鍵情報４４１には、

（ａ）鍵番号４４１ａとして、データブロック４０２のデータブロック番号４２２と等しい値が設定され、

（ｂ）鍵データ４４１ｂとして、データブロック４０２の鍵情報４４２と実行ブロック４５２とを復号化するための鍵データが設定され、

（ｃ）暗号化有無情報４４１ｃとして、実行ブロック４５２が暗号化されている

ことを示す値（例えば０ｘ１０）が設定される。

【００６３】

また、もう一方の鍵情報４４１には、

（ａ）鍵番号４４１ａとして、データブロック４０３のデータブロック番号４２３と等しい値が設定され、

（ｂ）鍵データ４４１ｂとして、データブロック４０３の鍵情報４４３を復号化するための鍵データが設定され、

（ｃ）暗号化有無情報４４１ｃとして、実行ブロック４５３が暗号化されていないことを示す値（例えば０ｘ０１）が設定される。

【００６４】

なお、上記鍵情報４４１は、次に読み込まれる可能性があるデータブロックに対応するものだけでなく、例えば全てのデータブロックに対応するものを設けるようにして、後述するように鍵情報４４１を生成する際に、データブロックの読み込み順序の解析などをしなくてもよいようにしてもよい。

【００６５】

また、データブロック４０１の実行ブロック４５１は、一連の命令コードから成るプログラム（データ）が分割された、他のデータブロックへのデータブロック分岐命令を含む命令コード列によって構成されている。上記データブロック分岐命令は、具体的には、例えば図９に示すように、条件分岐命令５０１の後に、データブロック４０２・４０３への無条件データブロック分岐命令５０２が設けられ、上記条件分岐命令５０１により判定条件に応じて分岐した後に、データブロック４０２・４０３の何れかに制御が移行するようになっている（言い替えれば、次に何れのデータブロックに移行するかはあらかじめ定まっておらず、何れに移行する可能性もある。）。また、条件判断によって、直接、データブロック４０２・４０３に移行する条件データブロック分岐命令５０３や、データブロック４０１の内外に移行する条件データブロック内外分岐命令５０４を用いたりしてもよい。

【００６６】

上記のようなデータのメモリ１２０への格納は、例えば、前記実施の形態１（

図４）と同じように、図１０に示すようにして行うことができる。すなわち、図１０における（Ｓ３０１）（Ｓ３０２）（Ｓ３０５）および（Ｓ３０６）は、実質的に図４の（Ｓ１０１）（Ｓ１０２）（Ｓ１０５）および（Ｓ１０６）とほぼ同じである。（Ｓ３０３）では、各データブロック４０１～４０７にデータブロック番号４２１～４２７を割り当てる一方、命令コード列を解析して、各データブロック４０１～４０７から分岐する可能性のあるデータブロックを求め、分岐先のデータブロックに応じた鍵番号４４１ａ～４４７ａと鍵データ４４１ｂ～４４７ｂと暗号化有無情報４４１ｃ～４４７ｃとから鍵情報４４１～４４７を生成するとともに、上記割り当てられたデータブロック番号４２１～４２７、分岐先の数に等しい値の鍵データ数４３１～４３７、および鍵情報４４１～４４７を連結することにより、復号化情報４１１～４１７が生成される。また、（Ｓ３０４）では、各命令コード列に含まれる分岐命令のうち、他のデータブロックに分岐するものをデータブロック分岐命令に置換して実行ブロック４５１～４５７を生成し、これと復号化情報４１１～４１７とからデータブロック４０１～４０７が生成される。なお、上記のような分岐命令の置換を行わず、元のプログラムが生成される際に、あらかじめデータブロック分岐命令が用いられるようにしてもよい。

【００６７】

（メモリ１２０に記憶されたデータの読み込みと実行動作）

上記のようにメモリ１２０に記憶されたプログラムがマイクロコンピュータ３００に読み込まれて実行される場合の動作について、図１１に基づいて説明する。

【００６８】

（Ｓ４０１）　マイクロコンピュータ３００の外部から、最初に読み込まれるデータブロック、例えばデータブロック４０１についての鍵データ４４０ｂと、その鍵データ４４０ｂがデータブロック４０１に対するものであることを示す鍵番号４４０ａ（すなわちデータブロック４０１のデータブロック番号４２１に等しい値）と、暗号化された実行ブロック４５１が読み込まれる際に選択部３０４によって復号化部１０２の出力を選択することを示す選択指示とが入力されると

、これらを復号化情報管理部３０６の鍵テーブル３０６ａが保持する。

【００６９】

（Ｓ４０２）　復号化制御部３０１ａの制御によって、ＣＰＵ３０１が選択部３０４に例えばＨレベルのデータブロック番号・鍵データ数読み込み信号を出力すると、選択部３０４は、選択指示保持部１０５から出力される選択指示に係らず、メモリ１２０からの出力を直接選択するように切り替わる。

【００７０】

（Ｓ４０３）　復号化制御部３０１ａの制御によって、ＣＰＵ３０１が復号化情報におけるデータブロック番号と鍵データ数とを読み込むためのアドレス（および図示しない読み出し制御信号）を順次メモリ１２０に出力する。これに応じて、メモリ１２０はデータブロック番号と鍵データ数とを出力する。このデータブロック番号と鍵データ数とは、そのまま（復号化部１０２による復号化がなされることなく）選択部３０４を介してＣＰＵ３０１に入力される。

【００７１】

（Ｓ４０４）　ＣＰＵ３０１が上記データブロック番号を（図示しない出力タイミング信号と伴に）復号化情報管理部３０６に出力すると、制御部３０６ｂは、鍵テーブル３０６ａに保持された鍵番号のうち、上記データブロック番号に一致する鍵番号と対応して保持されている鍵データおよび選択指示をそれぞれ鍵データ保持部１０３または選択指示保持部１０５に出力して設定する。ここで、上記データブロック番号と鍵テーブル３０６ａに保持されている各鍵番号とが一致するかどうかの判定は、例えば、各鍵番号について並列に行わせるようにしてもよいし、一致するものが検出されるまで順次比較を行わせるようにしてもよい。ただし、特に後者の場合に、検出に要する時間が不定となる場合には、検出されたことを示す検出信号や鍵データ保持部１０３および選択指示保持部１０５への設定が完了したことを示す設定終了信号をＣＰＵ３０１に出力する一方、ＣＰＵ３０１は上記信号が入力されるまで鍵情報４４１の読み込み（アドレスの出力等）を開始しないようにすることが好ましい。

【００７２】

（Ｓ４０５）　ＣＰＵ３０１がデータブロック番号・鍵データ数読み込み信号

をＬレベル、鍵情報読み込み信号をＨレベルにし、選択部３０４は復号化部１０２の出力を選択するように切り替わる。

【００７３】

（Ｓ４０６）　ＣＰＵ３０１が上記鍵データ数に応じた数の鍵情報を順次メモリ１２０から選択部３０４を介して読み込み、鍵番号と、鍵データと、暗号化有無情報に応じた選択指示とを（図示しない出力タイミング信号と伴に）復号化情報管理部３０６に出力して、鍵テーブル３０６ａに保持させる。

【００７４】

（Ｓ４０７）　鍵データ数に応じた数の鍵情報についての処理が完了すると、ＣＰＵ３０１は鍵情報読み込み信号をＬレベルにする。そこで、選択部３０４は、選択指示保持部１０５に設定されている選択指示に基づいて、復号化部１０２の出力またはメモリ１２０の出力を選択的にＣＰＵ３０１に入力するように切り替わる。

【００７５】

（Ｓ４０８）　ＣＰＵ３０１が実行ブロックの各命令コードに応じたアドレスを出力し、メモリ１２０から出力された命令コードは、選択部３０４を介し、暗号化の有無に応じて、すなわち暗号化されている場合には復号化部１０２により復号化された後、または平文である場合にはそのまま、ＣＰＵ３０１に入力される。

【００７６】

（Ｓ４０９）　ＣＰＵ３０１に入力された命令コードの命令がデータブロック分岐命令であれば、（Ｓ４０２）に戻って次のデータブロックについて同じ処理が繰り返される。

【００７７】

（Ｓ４１０）　一方、データブロック分岐命令でなければ、ＣＰＵ３０１は読み込まれた命令コードの命令を実行し、データブロック分岐命令が読み込まれるまで、（Ｓ４０８）～（Ｓ４１０）を繰り返す。

【００７８】

上記のように、各データブロックに分岐先のデータブロックに応じた１つ以上

の鍵データを含めることにより、データブロックの読み込み順序が一定でない場合でも適切に各データブロックの内容を読み込むことができるので、実施の形態１と同様に記憶内容の秘匿性を高められることに加えて、プログラムの作成や分割を柔軟に行うことが容易にできる。

【００７９】

なお、上記のように各データブロックに、分岐先となる可能性のあるデータブロック用の鍵データを（暗号化して）含めるのに代えて、分岐先となるデータブロックに、そのデータブロック用の複数の同一の鍵データが、それぞれ、そのデータブロックに分岐してくる分岐元となる可能性のあるデータブロックと同じように暗号化されたものを含めるようにしてもよい。すなわち、分岐先のデータブロックで読み込まれた複数の暗号化された鍵データのうち、分岐元のデータブロックに対応するものが、分岐元のデータブロックと同じ鍵データを用いて復号化されるようにすれば、そのデータブロック用の適切な鍵データを得ることができる。

【００８０】

（実施の形態３）

上記実施の形態２と同様に、任意の順序でデータブロックを読み込ませることができるマイクロコンピュータの他の例について説明する。

【００８１】

（メモリ１２０に記憶されるデータの形式）

まず、このマイクロコンピュータで読み込まれるデータがメモリ１２０に記憶される形式について、図１２に基づいて説明する。メモリ１２０には、複数の（例えば３つの）データブロック７０１～７０３が記憶され、各データブロック７０１～７０３は、復号化情報７１１’～７１３’と、実行ブロック７２１～７２３とから構成されている。上記実行ブロック７２１～７２３は、実施の形態１と同様に、一連の命令コードから成るプログラム（データ）が３つの実行単位に分割された命令コード列７２１ａ～７２３ａに実行終了コード２３０が付加されて構成され、必要に応じて（例えば実行ブロック７２１が）暗号化されている。

【００８２】

上記暗号化された実行ブロック７２１を含むデータブロック７０１の復号化情報７１１’は、上記実行ブロック７２１を復号化するための鍵データ７１１が所定の共通鍵データ７４０により暗号化されたものである。一方、暗号化されていない実行ブロック７２２・７２３を含むデータブロック７０２・７０３の復号化情報７１２’・７１３’は、所定のダミー鍵データ７１０が、データブロック７０１と同じ共通鍵データ７４０により暗号化されたものである。（なお、復号化情報７１１’～７１３’には、前記実施の形態１、２のように暗号化有無情報は含まれていないが、この点については後述する。）上記共通鍵データ７４０は、特に限定されないが、システムごとに異ならせると、データの秘匿性をより高めることが容易にできる。また、上記共通鍵データ７４０による鍵データ７１１の暗号化の手法も、実行ブロック７２１と同様に、共通鍵暗号方式など種々の手法を適用することができる。

【００８３】

（装置の構成）

上記のような記憶内容を読み込むマイクロコンピュータ６００は、図１３に示すように、実施の形態１（図１）のマイクロコンピュータ１００と比べて、ＣＰＵ１０１、選択部１０４、および復号化情報管理部１０６に代えて、ＣＰＵ６０１、選択部６０４、および復号化情報管理部６０６を備えている点が異なっている。

【００８４】

ＣＰＵ６０１に設けられる復号化制御部６０１ａと実施の形態１の復号化制御部１０１ａとの相違は、上記のようにメモリ１２０に記憶されるデータブロックの形式が実施の形態１とは異なることに対応するものである。

【００８５】

選択部６０４は、例えばＨレベルの復号化情報読み込み信号が入力される場合には、選択指示保持部１０５に設定された選択指示に係らず、メモリ１２０の出力を選択するようになっている。

【００８６】

復号化情報管理部６０６は、鍵データ復号化部６０６ａ（第２の復号化部）と

、共通鍵データ保持部６０６ｂ（第２の鍵データ保持部）と、暗号化有無判定部６０６ｃと、比較データ保持部６０６ｄとを備えている。

【００８７】

鍵データ復号化部６０６ａは、ＣＰＵ６０１がメモリ１２０から読み込んで出力した復号化情報７１１’～７１３’（暗号化された鍵データ７１１またはダミー鍵データ７１０）を復号化して、元の鍵データ７１１またはダミー鍵データ７１０を出力するようになっている。上記鍵データの復号化には、マイクロコンピュータ６００の外部から入力されて共通鍵データ保持部６０６ｂに保持された共通鍵データ７４０が用いられる。

【００８８】

暗号化有無判定部６０６ｃは、上記鍵データ復号化部６０６ａの出力と、マイクロコンピュータ６００の外部から入力されて比較データ保持部６０６ｄに保持されたダミー鍵データ７１０とを比較し、一致する場合には、選択部６０４にメモリ１２０からの出力を選択させる選択指示を出力する一方、一致しない場合には、復号化部１０２（第１の復号化部）からの出力を選択させる選択指示を出力するようになっている。すなわち、実行ブロック７２２・７２３が暗号化されていないデータブロック７０２・７０３の復号化情報７１２’・７１３’が復号化されると鍵データ復号化部６０６ａからはダミー鍵データ７１０が出力されるので、これと、比較データ保持部６０６ｄに保持されているダミー鍵データ７１０とが一致すると判定されることによって、実行ブロック７２２・７２３が暗号化されていないことを判別でき、選択部６０４にメモリ１２０の出力を選択させることができる。（なお、この場合、鍵データ保持部１０３（第１の鍵データ保持部）に上記ダミー鍵データ７１０が保持されたとしても、復号化部１０２の出力は選択部６０４によって選択されないので、ＣＰＵ６０１に入力されるデータには影響がない。）

前記のようなデータのメモリ１２０への格納は、例えば図１４に示すようにして行うことができる。同図において、（Ｓ５０２）（Ｓ５０５）（Ｓ５０７）は、実質的に前記実施の形態１（図４）の（Ｓ１０１）（Ｓ１０４）（Ｓ１０６）とほぼ同じである。（Ｓ５０１）では、データブロック７０１～７０３の復号化

情報７１１’～７１３’を復号化して鍵データ７１１またはダミー鍵データ７１０を得るための共通鍵データ７４０を決定し、（Ｓ５０３）では、データブロック７０１用の鍵データ７１１を決めるとともにデータブロック７０２・７０３用のダミー鍵データ７１０を決め、（Ｓ５０４）では、鍵データ７１１およびダミー鍵データ７１０が共通鍵データ７４０で暗号化されて復号化情報７１１’～７１３’が得られる。また、（Ｓ５０６）では、実行ブロック７２１だけが鍵データ７１１によって暗号化される。

【００８９】

（メモリ１２０に記憶されたデータの読み込みと実行動作）

上記のようにメモリ１２０に記憶されたプログラムがマイクロコンピュータ６００に読み込まれて実行される場合の動作について、図１５に基づいて説明する。

【００９０】

（Ｓ６０１）　マイクロコンピュータ６００の外部から、共通鍵データ７４０、およびダミー鍵データ７１０が入力されると、これらを復号化情報管理部６０６の共通鍵データ保持部６０６ｂ、および比較データ保持部６０６ｄが保持する。

【００９１】

（Ｓ６０２）　復号化制御部６０１ａの制御によって、ＣＰＵ６０１が選択部６０４に例えばＨレベルの復号化情報読み込み信号を出力すると、選択部６０４は、選択指示保持部１０５から出力される選択指示に係らず、メモリ１２０からの出力を直接選択するように切り替わる。

【００９２】

（Ｓ６０３）　復号化制御部６０１ａの制御によって、ＣＰＵ６０１がメモリ１２０に復号化情報を読み込むためのアドレス（および図示しない読み出し制御信号）を出力する。これに応じて、メモリ１２０は復号化情報を出力する。この復号化情報は、そのまま（復号化部１０２による復号化がなされることなく）選択部６０４を介してＣＰＵ６０１に入力される。ここで、復号化情報が復号化部１０２によって復号化されないのは、後に鍵データ復号化部６０６ａによって復

号化されるからである。

【００９３】

（Ｓ６０４）　ＣＰＵ６０１は、入力された復号化情報を復号化情報管理部６０６の鍵データ復号化部６０６ａに（図示しない出力タイミング信号と伴に）出力する。

【００９４】

（Ｓ６０５）　鍵データ復号化部６０６ａが、共通鍵データ保持部６０６ｂに保持されている共通鍵データ７４０を用いて、ＣＰＵ６０１から入力された復号化情報を復号化し、得られた鍵データ７１１（またはダミー鍵データ７１０）を鍵データ保持部１０３に設定するとともに、暗号化有無判定部６０６ｃにも出力する。

【００９５】

（Ｓ６０６）　暗号化有無判定部６０６ｃは鍵データ復号化部６０６ａの出力と比較データ保持部６０６ｄに保持されているダミー鍵データ７１０と比較し、一致する場合には、選択部６０４にメモリ１２０からの出力を選択させる選択指示を出力する一方、一致しない場合には、復号化部１０２からの出力を選択させる選択指示を出力して、選択指示保持部１０５に設定する。すなわち、鍵データ復号化部６０６ａによって復号化されたのがダミー鍵データ７１０であれば、そのデータブロックの実行ブロックは暗号化されていないので、選択部６０４にメモリ１２０からの出力を選択させ、そのままＣＰＵ６０１に入力させるようにする。また、鍵データ復号化部６０６ａによって復号化されたのがダミー鍵データ７１０でなければ、それは鍵データなので、選択部６０４に復号化部１０２の出力を選択させ、上記（Ｓ６０５）で鍵データ保持部１０３に設定された鍵データ７１１を用いて復号化されたデータをＣＰＵ６０１に入力させるようにする。

【００９６】

（Ｓ６０７）　ＣＰＵ６０１から出力される復号化情報読み込み信号がＬレベルになると、選択部６０４は、選択指示保持部１０５に設定されている選択指示に基づいて、復号化部１０２の出力またはメモリ１２０の出力を選択的にＣＰＵ６０１に入力するように切り替わる。

【００９７】

（Ｓ６０８）　ＣＰＵ６０１が実行ブロックの各命令コードに応じたアドレスを出力し、メモリ１２０から出力された命令コードは、選択部６０４を介し、暗号化の有無に応じて、すなわち暗号化されている場合には復号化部１０２により復号化された後、または平文である場合にはそのまま、ＣＰＵ６０１に入力される。

【００９８】

（Ｓ６０９）　メモリ１２０から出力されたのが実行終了コード２３０であれば、（Ｓ６０２）に戻って次のデータブロックについて同じ処理が繰り返される。

【００９９】

（Ｓ６１０）　一方、メモリ１２０から出力されたのが実行終了コード２３０でなければ、ＣＰＵ６０１は読み込まれた命令コードの命令を実行し、実行終了コード２３０が読み込まれるまで、（Ｓ６０８）～（Ｓ６１０）を繰り返す。

【０１００】

上記のように、各実行ブロックを復号化する鍵データを、各実行ブロックと同じデータブロックに含めることにより、上記鍵データの取得はデータブロックの読み込み順序に依存しないので、任意の順序で読み込むことができる。また、マイクロコンピュータ６００の外部から与える必要のある（管理する必要のある）鍵データは、（各実行ブロックを復号化するための鍵データを復号化する）上記共通鍵データだけなので、やはり、鍵データの管理の簡素化を図ることができる。ここで、上記共通鍵データが万一漏洩すると複数の鍵データが解読される可能性はあるが、これによって知られてしまうのはあくまで鍵データだけであり、記憶データを取得するためには、さらにその鍵データを用いた復号化を行わなければならない。そして、そのためには、鍵データの他に暗号化アルゴリズム、各データブロック７０１～７０３の区切りや復号化情報７１１’～７１３’と実行ブロック７２１との区切り、復号化情報７１１’～７１３’の配置なども知る必要があるので、メモリ１２０の記憶内容を解読することはやはり非常に困難であり、実際上、記憶内容の漏洩を防止することが容易にできる。

【０１０１】

なお、上記の例では、暗号化有無判定部６０６ｃが鍵データ復号化部６０６ａの出力を比較データ保持部６０６ｄの出力と比較する例を示したが、鍵データ保持部１０３の出力を比較するようにしてもよい。この場合には、鍵データ保持部１０３に同じ値が保持されている間は、暗号化有無判定部６０６ｃからの出力も同じに保たれるので、選択指示保持部１０５を省略することができる。

【０１０２】

さらに、ＣＰＵ６０１から出力される（鍵データ復号化部６０６ａによる復号化前の）復号化情報７１１’～７１３’を比較データ保持部６０６ｄの出力と比較するようにしてもよい。この場合には、データブロック７０１～７０３の復号化情報７１２’・７１３’を生成する際にダミー鍵データ７１０を暗号化しなくてもよい。

【０１０３】

また、上記の例では、復号化情報７１１’～７１３’の復号化を鍵データ復号化部６０６ａが行い、実行ブロック７２１～７２３の復号化を復号化部１０２が行うように構成された例を示したが、これに限らず、例えばそれぞれの復号化を行う際に、共通鍵データ７４０または鍵データ７１１を鍵データ保持部１０３に設定するようにして、何れの復号化も復号化部１０２によって行わせるようにしてもよい。このように復号化部を兼用することにりハードウェア規模を小さく抑えることができる。一方、前記のように復号化部を分けて設ける場合には、兼用する場合に比べて、それぞれの復号化に互いに異なるアルゴリズムを用いるようにすることが容易にできる。特に、鍵データの復号化は各データブロックについて１回行うだけなので、マイクロコンピュータ６００の処理時間に大きな影響を与えることなく、暗号強度の高い暗号化方式を適用することなども容易にできる。

【０１０４】

ここで、例えば、鍵データ復号化部６０６ａの復号化に要するクロックサイクルが、ループ処理などによって複数クロックになる場合や不定である場合などには、鍵データ復号化部６０６ａによる復号化が完了して鍵データ保持部１０３に

鍵データが設定されるタイミングで復号化情報管理部６０６から設定終了信号を出力させ、これがＣＰＵ６０１に入力されるまでの間、ＣＰＵ６０１に次のアドレス出力等のデータの読み込み動作を停止させるようにすれば、復号化部１０２によって復号化されたデータを確実にＣＰＵ６０１に入力させることが容易にできる。

【０１０５】

（実施の形態４）

上記実施の形態３の変形例で説明したようにＣＰＵ６０１がメモリ１２０から読み込んだ復号化情報７１１’～７１３’を鍵データ復号化部６０６ａに出力した後、鍵データ復号化部６０６ａによる復号化が完了して鍵データ７１１が鍵データ保持部１０３に設定されるまでの間にＣＰＵ６０１の動作を停止させる場合、マイクロコンピュータ３００とメモリ１２０との間で送受される信号を監視すれば、マイクロコンピュータ６００が通常のメモリアクセスをしている場合とは異なる動作をしていると推測しやすくなる。そこで、もし、メモリ１２０の記憶内容を不正に取得しようとする者によって、アドレスが出力されない期間にＣＰＵ６０１の内部で復号化処理がなされていると推測されたとすると、その直前に出力されたアドレスの領域に着目されやすくなる。その場合でも、その着目された領域に鍵データが記憶されているとは限らず、また、前記のように暗号化アルゴリズム等が判らなければ、メモリ１２０の記憶内容の解読は困難であることに変わりないが、上記のように特定の領域に着目されるようなことも起こりにくいようにするために、疑似的なアドレスをマイクロコンピュータ６００から出力させるようにしてもよい。

【０１０６】

具体的には、例えば図１６に示すマイクロコンピュータ８００は、実施の形態３のマイクロコンピュータ６００（図１３）と比べて、ＣＰＵ６０１と、復号化情報管理部６０６とに代えて、ＣＰＵ６０１’と、鍵データ復号化部６０６ａ’を有する復号化情報管理部６０６’とを備えるとともに、さらに、擬似アドレス発生部８１１（擬似読み込み信号出力部）を備えている点が異なっている。

【０１０７】

上記鍵データ復号化部６０６ａ’は、復号化が完了して鍵データ保持部１０３に鍵データが設定されるタイミングで、例えばＨレベルの設定終了信号をＣＰＵ６０１’に出力するようになっている。

【０１０８】

ＣＰＵ６０１’は、基本的な動作はＣＰＵ６０１と同じであるが、復号化情報管理部６０６’の鍵データ復号化部６０６ａ’によって、暗号化された鍵データが復号化される間（すなわち、復号化情報７１１’～７１３’と伴に例えばＨレベルの出力タイミング信号を鍵データ復号化部６０６ａ’に出力してから、Ｈレベルの設定終了信号が鍵データ復号化部６０６ａ’からＣＰＵ６０１’に入力されるまでの間）、次のアドレス出力等のデータの読み込み動作を停止するようになっている。

【０１０９】

擬似アドレス発生部８１１は、ＣＰＵ６０１’から出力される復号化情報７１１’～７１３’の出力タイミング信号がＨレベルになってから、鍵データ復号化部６０６ａ’から出力される設定終了信号がＨレベルになるまでの間に、疑似的なアドレスを出力するようになっている。より詳しくは、ＣＰＵ６０１’から出力される出力タイミング信号がＨレベルになると、乱数生成部８１１ａは乱数を発生してインクリメント部８１１ｂに初期値として設定し（保持させ）、インクリメント部８１１ｂは、図示しないクロック信号に応じて、保持している値を順次インクリメントし、擬似アドレスとして出力するようになっている。また、出力制御部８１１ｃは、上記出力タイミング信号がＨレベルになってから、設定終了信号がＨレベルになるまでの間は、上記インクリメント部８１１ｂから出力される値（および図示しない読み出し制御信号）を出力する一方、その他の場合には、ＣＰＵ６０１’から出力されるアドレスをそのまま出力するようになっている。（上記のように擬似アドレスが出力されると、メモリ１２０からは無効なデータが出力されることになるが、その際、ＣＰＵ６０１’は上記のようにデータの読み込み動作を停止しているので、そのような無効なデータはＣＰＵ６０１’に取り込まれない。）

なお、上記各実施の形態では、メモリ１２０の記憶内容がプログラムである例

を示したが、これに限らず、所定のプログラム（読み込みプログラム）の実行によって読み込まれる単なるデータなどが、同様に分割、暗号化されて記憶されるようにしてもよい。その場合、各データブロックの読み込み順序は、上記読み込みプログラムによってあらかじめ定められていてもよいし、データブロック中に含められたポインタや管理情報などによって制御されるようにしてもよい。すなわち、何れの場合でも、どのデータブロックの次にどのデータブロックが読み込まれるかが定まっていて、それに応じた鍵データが各データブロックに含められるなどされていればよい。ここで、上記のように単なるデータが暗号化されて記憶されている場合、これを読み込む読み込みプログラムも同様に暗号化すれば、より秘匿性を高くすることができるが、読み込みプログラムを暗号化しなくても、これによって読み込まれる内容自体の解読は、やはり相当に困難なものにすることができる。

【０１１０】

また、上記の例では、鍵データ保持部１０３に設定される鍵データなどの初期値がマイクロコンピュータ１００の外部から入力される例を示したが、これに限らずマイクロコンピュータ１００の内部にあらかじめ設定された値などが用いられるようにしてもよい。

【０１１１】

また、図３等に示したデータ構造は論理的なもので、必ずしもメモリ１２０における物理的な記憶領域の関係が同図に示すようになっている必要はない。

【０１１２】

また、上記各実施の形態や変形例で説明した構成要素等は、それぞれ論理的に可能な範囲で、種々組み合わせてもよい。具体的には、例えば、実施の形態２～４において、実施の形態１の変形例で説明したように、選択部を設けず、全ての実行ブロックが暗号化されたデータブロックを読み込むようにしたり、実施の形態１、２において、選択部の切り替えを暗号化有無情報に基づいて行うのに代えて、実施の形態３、４で説明したようにダミー鍵データを用いて行うようにしたり、または逆に、実施の形態３、４において暗号化有無情報に基づいて切り替えるようにしたり、また、実施の形態１、２において、各復号化情報に含まれる鍵

データが実施の形態３、４と同様に共通鍵データによって復号化されるようにしたりしてもよい。

【０１１３】

【発明の効果】

以上のように本発明によると、記憶媒体に記憶されるべきデータを複数に分割して、それぞれ互いに異なる鍵データによって復号化されるように暗号化するとともに、上記鍵データも、それぞれ他の鍵データによって復号化されるように暗号化して記憶媒体に記憶させ、その記憶内容を読み込む際に、暗号化された鍵データから復号化された鍵データを用いて、暗号化されたデータおよび次の鍵データの復号化を順次行うようにすることにより、第三者が記憶媒体の記憶内容を不正に取得することの困難性を高めることができるとともに、複数の鍵データを管理する必要がなく、したがって、暗号鍵の管理の複雑化などを招くことなく、記憶媒体に記憶されたデータが容易に第三者に漏洩するのを防止可能にすることができる。

【図面の簡単な説明】

【図１】

実施の形態１のマイクロコンピュータ１００の要部の構成を示すブロック図である。

【図２】

同、メモリ１２０の記憶内容の例を示す説明図である。

【図３】

同、データブロック２０１のデータ構造の例を示す説明図である。

【図４】

同、メモリ１２０へのデータの格納手順の例を示すフローチャートである。

【図５】

同、メモリ１２０に記憶されたプログラムがマイクロコンピュータ１００に読み込まれて実行される場合の動作を示すフローチャートである。

【図６】

実施の形態２のマイクロコンピュータ３００の要部の構成を示すブロック図で

ある。

【図７】

同、鍵テーブル３０６ａの保持内容の例を示す説明図である。

【図８】

同、データブロック４０１のデータ構造の例を示す説明図である。

【図９】

同、命令コード列中のデータブロック分岐命令の例を示す説明図である。

【図１０】

同、メモリ１２０へのデータの格納手順の例を示すフローチャートである。

【図１１】

同、メモリ１２０に記憶されたプログラムがマイクロコンピュータ３００に読み込まれて実行される場合の動作を示すフローチャートである。

【図１２】

実施の形態３のデータブロック７０１のデータ構造の例を示す説明図である。

【図１３】

同、マイクロコンピュータ６００の要部の構成を示すブロック図である。

【図１４】

同、メモリ１２０へのデータの格納手順の例を示すフローチャートである。

【図１５】

同、メモリ１２０に記憶されたプログラムがマイクロコンピュータ６００に読み込まれて実行される場合の動作を示すフローチャートである。

【図１６】

実施の形態４のマイクロコンピュータ８００の要部の構成を示すブロック図である。

【符号の説明】

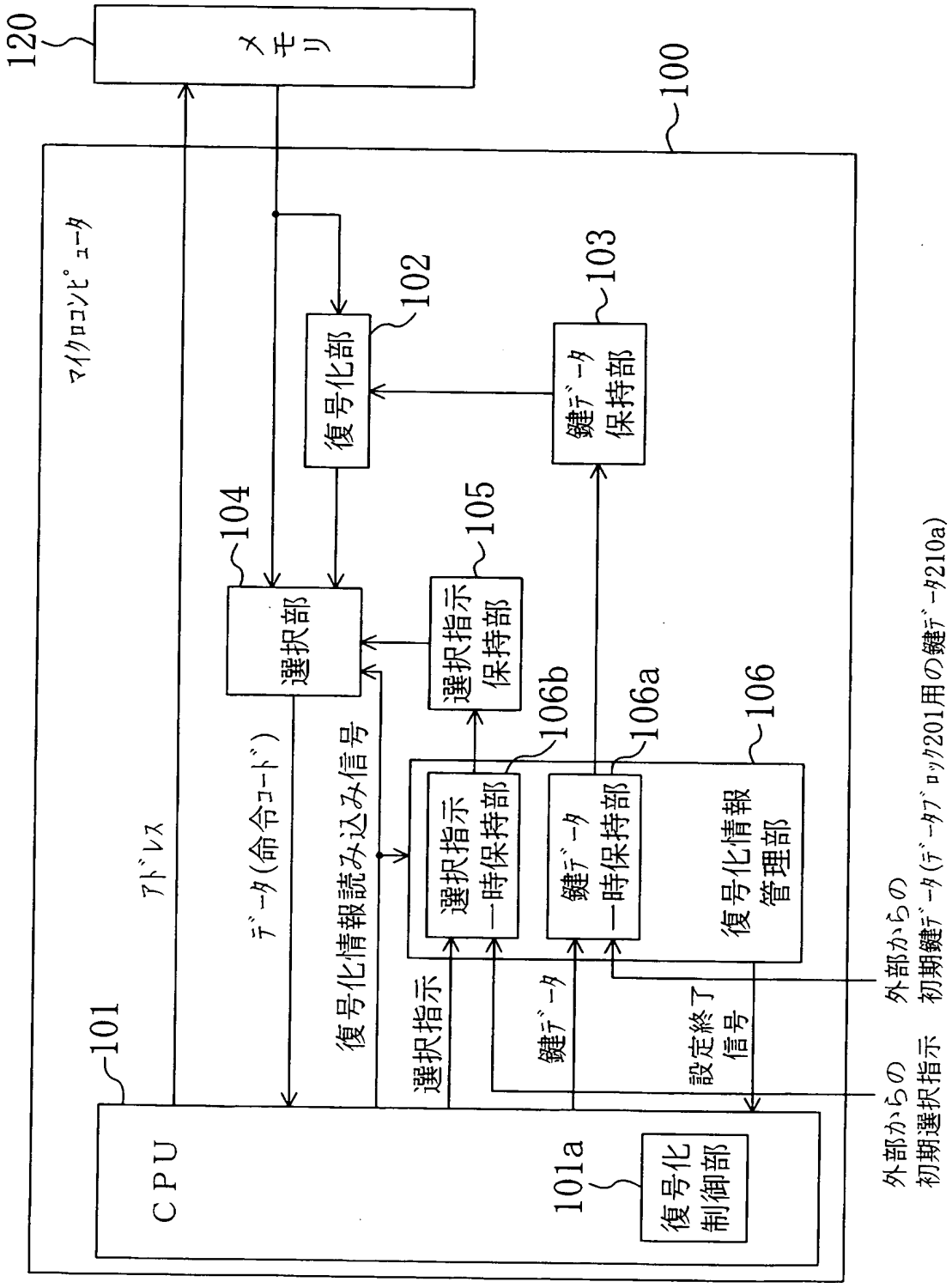
１００	マイクロコンピュータ
１０１	ＣＰＵ
１０１ａ	復号化制御部
１０２	復号化部

１０３　　鍵データ保持部
１０４　　選択部
１０５　　選択指示保持部
１０６　　復号化情報管理部
１０６ａ　　鍵データ一時保持部
１０６ｂ　　選択指示一時保持部
１２０　　メモリ
２０１～２０５　　データブロック
２１１～２１５　　復号化情報
２１０ａ～２１５ａ　　鍵データ
２１１ｂ～２１５ｂ　　暗号化有無情報
２２１～２２５　　実行ブロック
２２１ａ～２２５ａ　　命令コード列
２３０　　実行終了コード
３００　　マイクロコンピュータ
３０１　　ＣＰＵ
３０１ａ　　復号化制御部
３０４　　選択部
３０６　　復号化情報管理部
３０６ａ　　鍵テーブル
３０６ｂ　　制御部
４０１～４０７　　データブロック
４１１～４１７　　復号化情報
４２１～４２７　　データブロック番号
４３１～４３７　　鍵データ数
４４１～４４７　　鍵情報
４４０ａ～４４７ａ　　鍵番号
４４０ｂ～４４７ｂ　　鍵データ
４４１ｃ～４４７ｃ　　暗号化有無情報

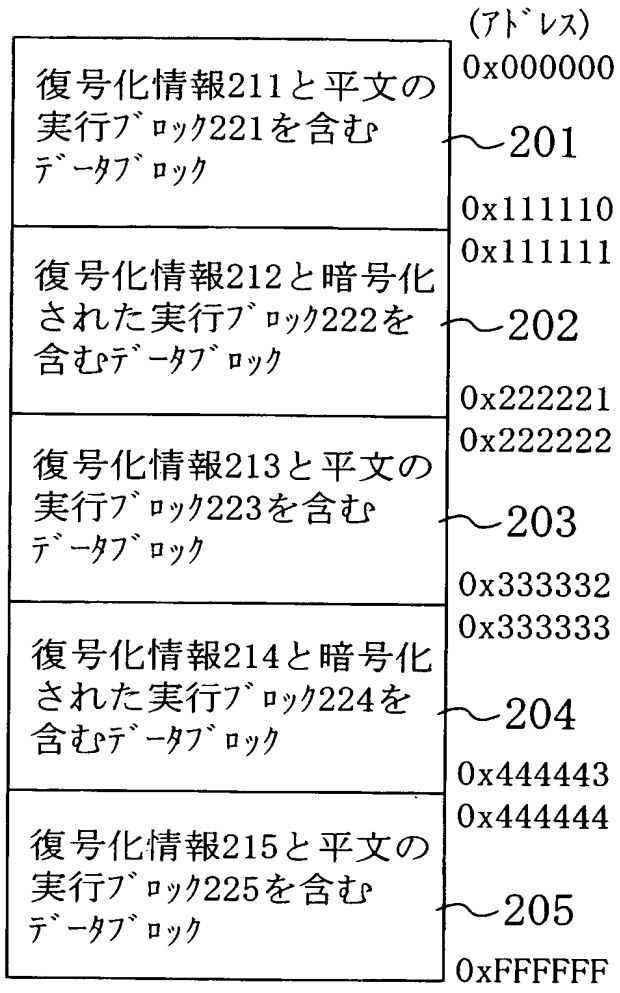
４５１～４５７　　実行ブロック
５０１　　条件分岐命令
５０２　　無条件データブロック分岐命令
５０３　　条件データブロック分岐命令
５０４　　条件データブロック内外分岐命令
６００　　マイクロコンピュータ
６０１　　ＣＰＵ
６０１’　　ＣＰＵ
６０１ａ　　復号化制御部
６０４　　選択部
６０６　　復号化情報管理部
６０６’　　復号化情報管理部
６０６ａ　　鍵データ復号化部
６０６ａ’　　鍵データ復号化部
６０６ｂ　　共通鍵データ保持部
６０６ｃ　　暗号化有無判定部
６０６ｄ　　比較データ保持部
７０１～７０３　　データブロック
７１０　　ダミー鍵データ
７１１　　鍵データ
７１１’～７１３’　　復号化情報
７２１～７２３　　実行ブロック
７２１ａ～７２３ａ　　命令コード列
７４０　　共通鍵データ
８００　　マイクロコンピュータ
８１１　　擬似アドレス発生部
８１１ａ　　乱数生成部
８１１ｂ　　インクリメント部
８１１ｃ　　出力制御部

【書類名】　図面

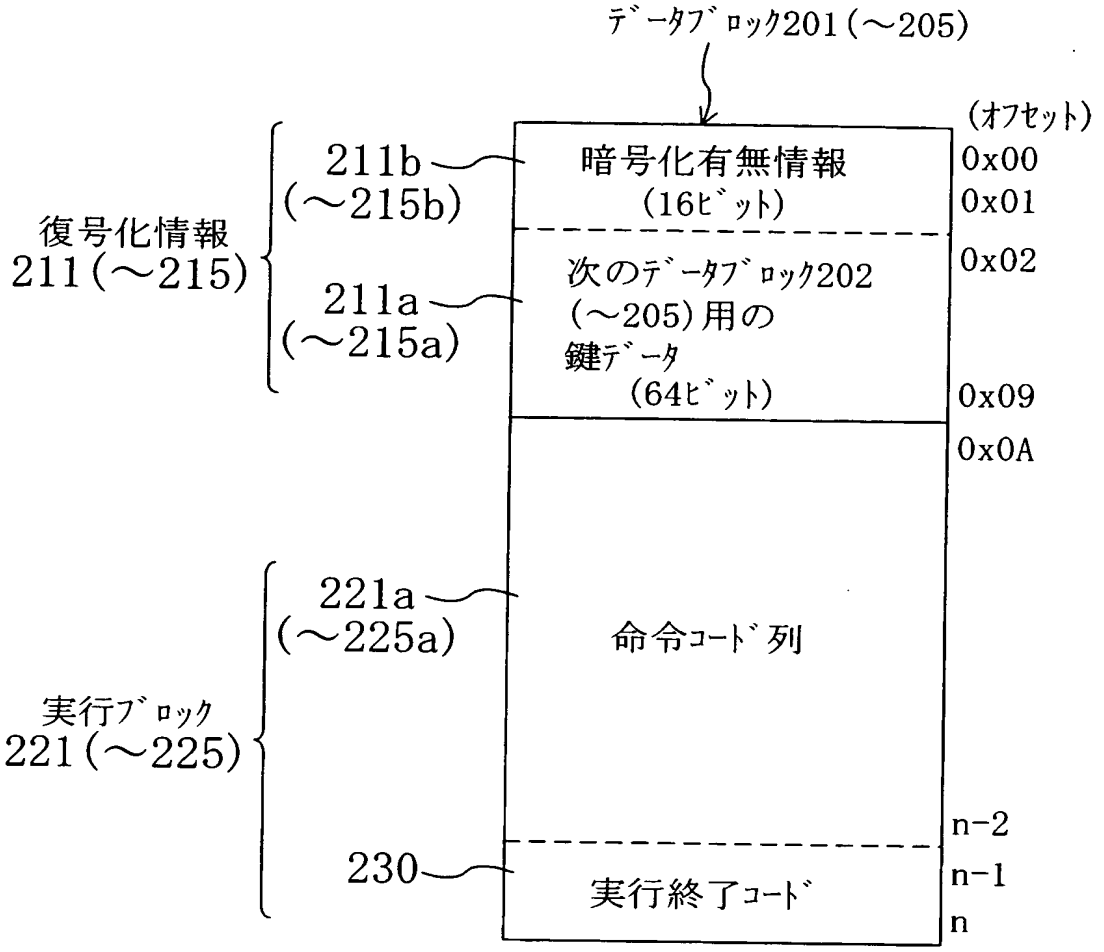
【図１】


120
メモリ
100
マイクロコンピュータ
102
復号化部
103
鍵データ保持部
104
選択部
105
選択指示保持部
106b
106a
106
選択指示一時保持部
鍵データ一時保持部
復号化情報管理部
101
CPU
101a
復号化制御部
アドレス
データ(命令コード)
復号化情報読み込み信号
選択指示
鍵データ
設定終了信号
外部からの初期選択指示
外部からの初期鍵データ(データブロック201用の鍵データ210a)

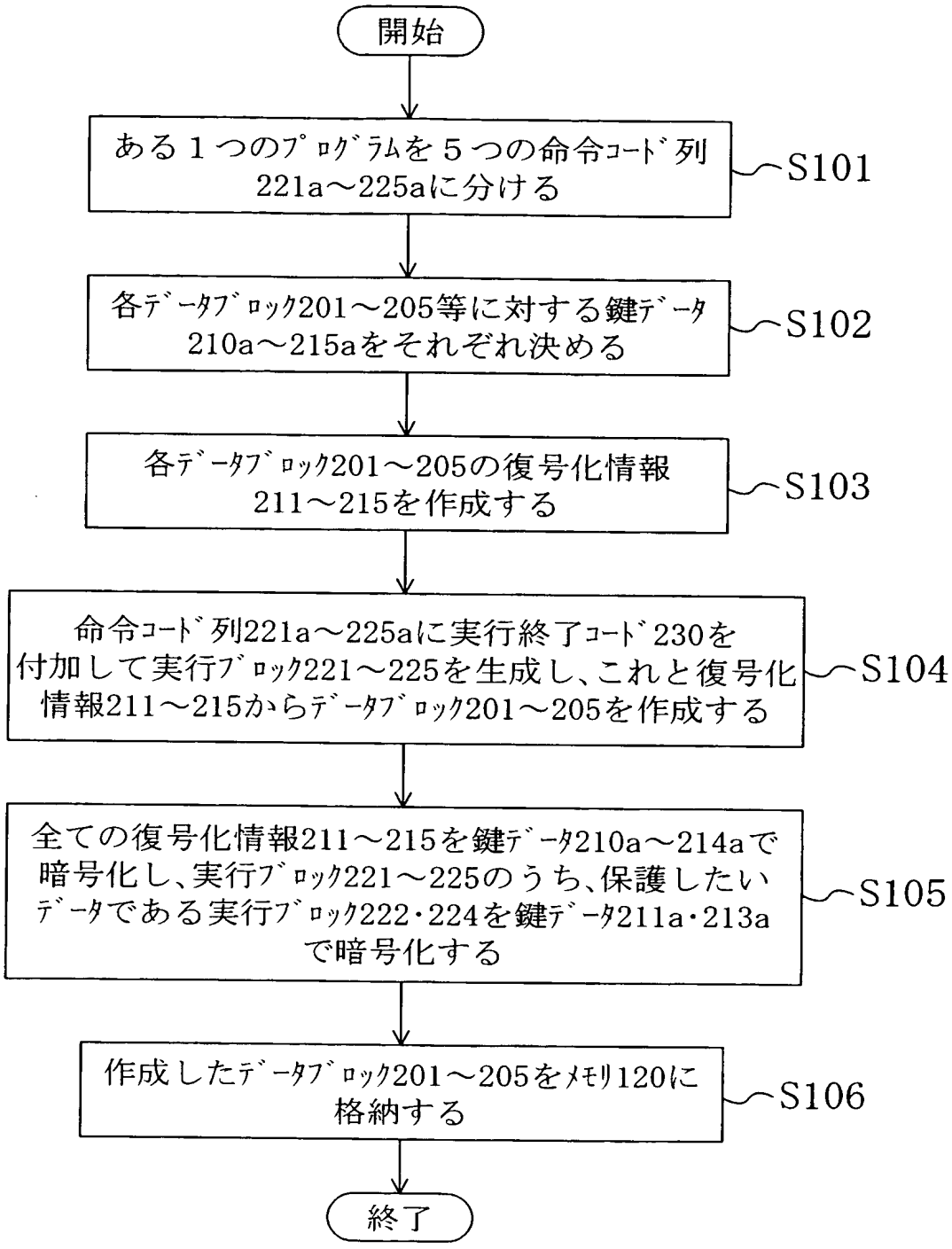
【図２】


メモリ120の記憶内容
(アドレス)
0x000000
復号化情報211と平文の実行ブロック221を含むデータブロック
201
0x111110
0x111111
復号化情報212と暗号化された実行ブロック222を含むデータブロック
202
0x222221
0x222222
復号化情報213と平文の実行ブロック223を含むデータブロック
203
0x333332
0x333333
復号化情報214と暗号化された実行ブロック224を含むデータブロック
204
0x444443
0x444444
復号化情報215と平文の実行ブロック225を含むデータブロック
205
0xFFFFFF

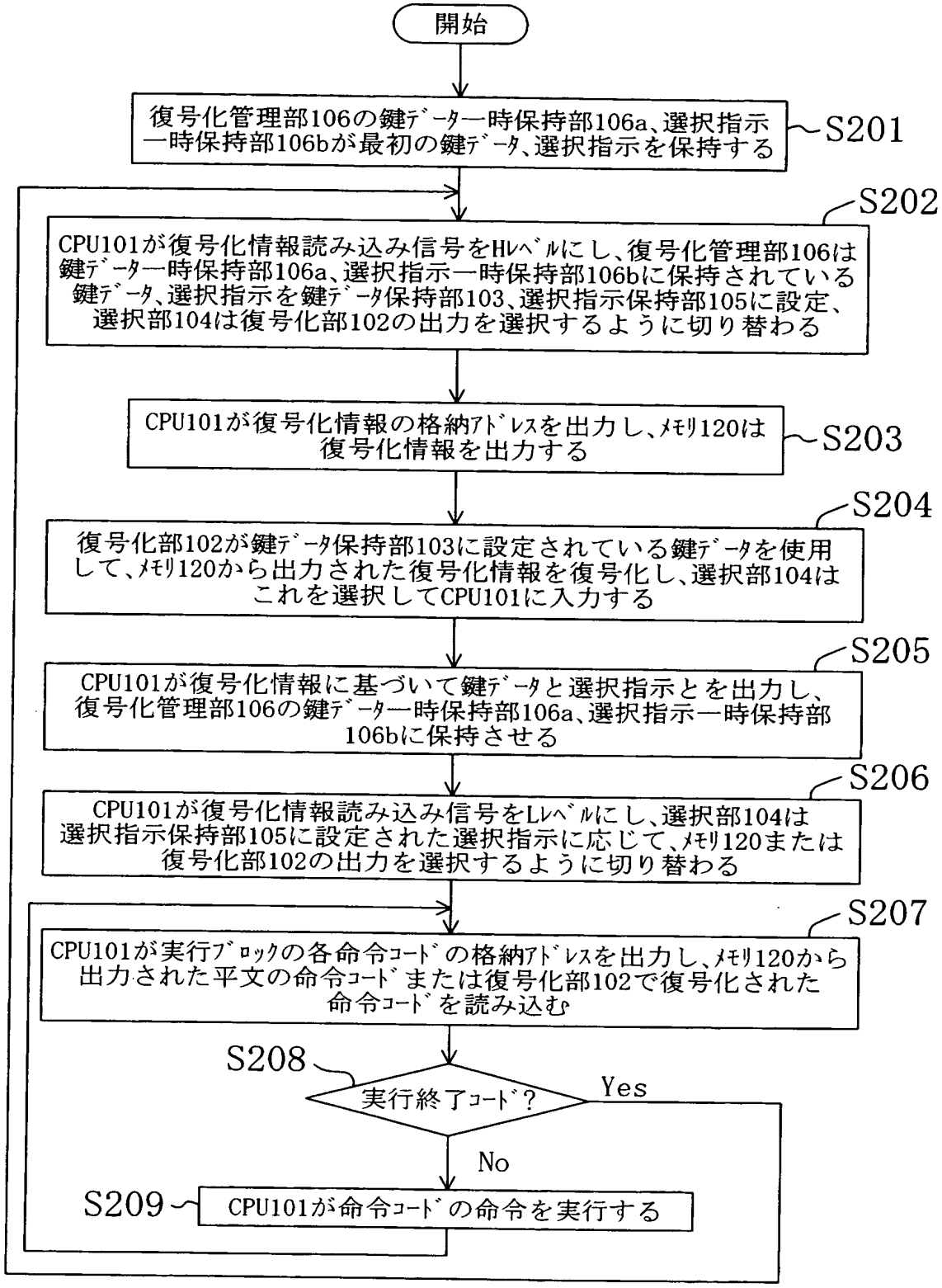
【図３】


データブロック201(～205)
(オフセット)
211b
(～215b)
暗号化有無情報
(16ビット)
0x00
0x01
復号化情報
211(～215)
211a
(～215a)
次のデータブロック202
(～205)用の
鍵データ
(64ビット)
0x02
0x09
0x0A
221a
(～225a)
命令コード列
実行ブロック
221(～225)
n-2
230
実行終了コード
n-1
n

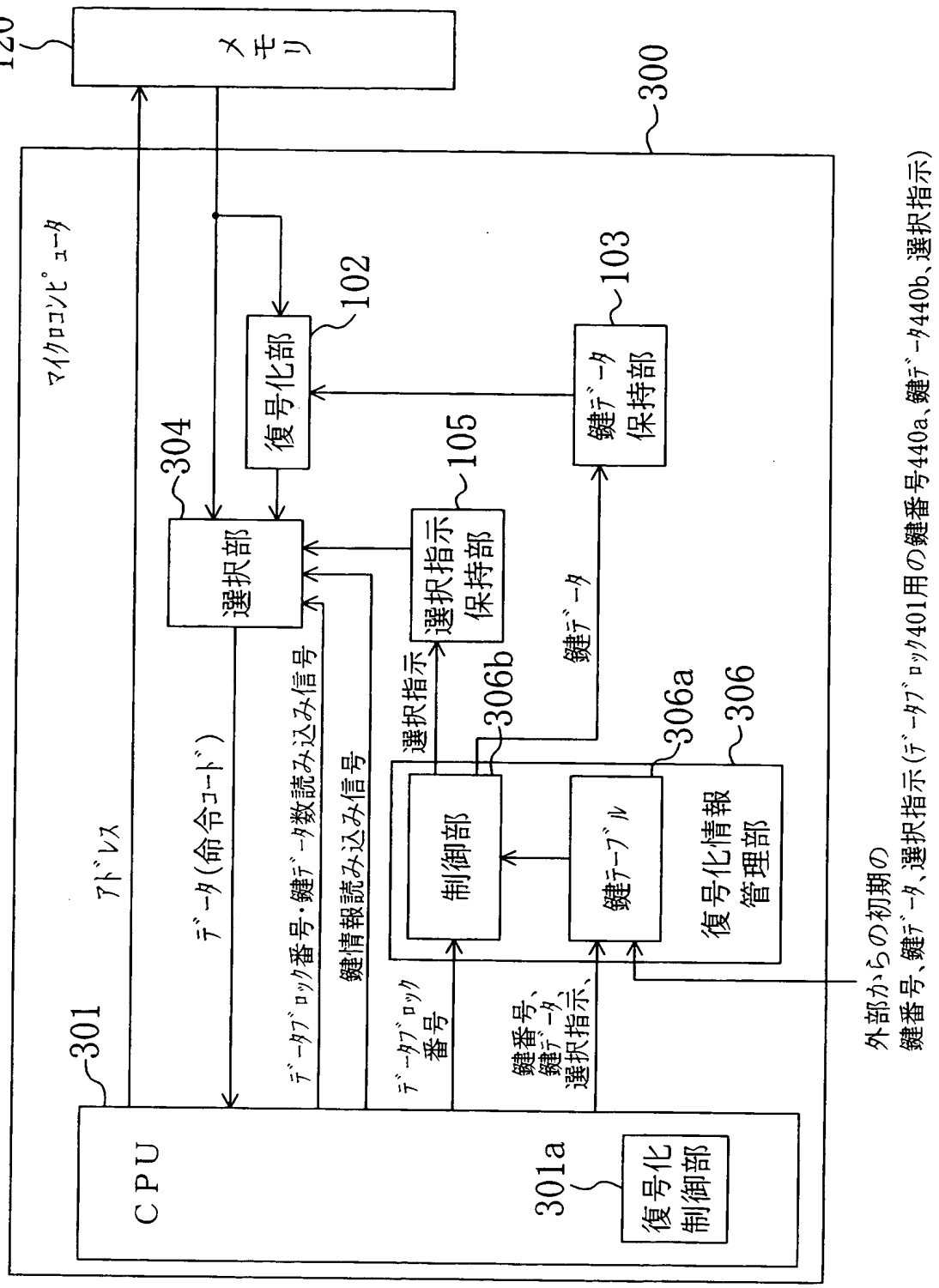
【図４】


開始
ある１つのﾌﾟﾛｸﾞﾗﾑを５つの命令ｺｰﾄﾞ列221a～225aに分ける
S101
各ﾃﾞｰﾀﾌﾞﾛｯｸ201～205等に対する鍵ﾃﾞｰﾀ210a～215aをそれぞれ決める
S102
各ﾃﾞｰﾀﾌﾞﾛｯｸ201～205の復号化情報211～215を作成する
S103
命令ｺｰﾄﾞ列221a～225aに実行終了ｺｰﾄﾞ230を付加して実行ﾌﾞﾛｯｸ221～225を生成し、これと復号化情報211～215からﾃﾞｰﾀﾌﾞﾛｯｸ201～205を作成する
S104
全ての復号化情報211～215を鍵ﾃﾞｰﾀ210a～214aで暗号化し、実行ﾌﾞﾛｯｸ221～225のうち、保護したいﾃﾞｰﾀである実行ﾌﾞﾛｯｸ222・224を鍵ﾃﾞｰﾀ211a・213aで暗号化する
S105
作成したﾃﾞｰﾀﾌﾞﾛｯｸ201～205をﾒﾓﾘ120に格納する
S106
終了

【図５】


開始
復号化管理部106の鍵ﾃﾞｰﾀ一時保持部106a、選択指示一時保持部106bが最初の鍵ﾃﾞｰﾀ、選択指示を保持する
S201
CPU101が復号化情報読み込み信号をHﾚﾍﾞﾙにし、復号化管理部106は鍵ﾃﾞｰﾀ一時保持部106a、選択指示一時保持部106bに保持されている鍵ﾃﾞｰﾀ、選択指示を鍵ﾃﾞｰﾀ保持部103、選択指示保持部105に設定、選択部104は復号化部102の出力を選択するように切り替わる
S202
CPU101が復号化情報の格納ｱﾄﾞﾚｽを出力し、ﾒﾓﾘ120は復号化情報を出力する
S203
復号化部102が鍵ﾃﾞｰﾀ保持部103に設定されている鍵ﾃﾞｰﾀを使用して、ﾒﾓﾘ120から出力された復号化情報を復号化し、選択部104はこれを選択してCPU101に入力する
S204
CPU101が復号化情報に基づいて鍵ﾃﾞｰﾀと選択指示とを出力し、復号化管理部106の鍵ﾃﾞｰﾀ一時保持部106a、選択指示一時保持部106bに保持させる
S205
CPU101が復号化情報読み込み信号をLﾚﾍﾞﾙにし、選択部104は選択指示保持部105に設定された選択指示に応じて、ﾒﾓﾘ120または復号化部102の出力を選択するように切り替わる
S206
CPU101が実行ﾌﾞﾛｯｸの各命令ｺｰﾄﾞの格納ｱﾄﾞﾚｽを出力し、ﾒﾓﾘ120から出力された平文の命令ｺｰﾄﾞまたは復号化部102で復号化された命令ｺｰﾄﾞを読み込む
S207
S208
実行終了ｺｰﾄﾞ？
Yes
No
S209
CPU101が命令ｺｰﾄﾞの命令を実行する

【図６】

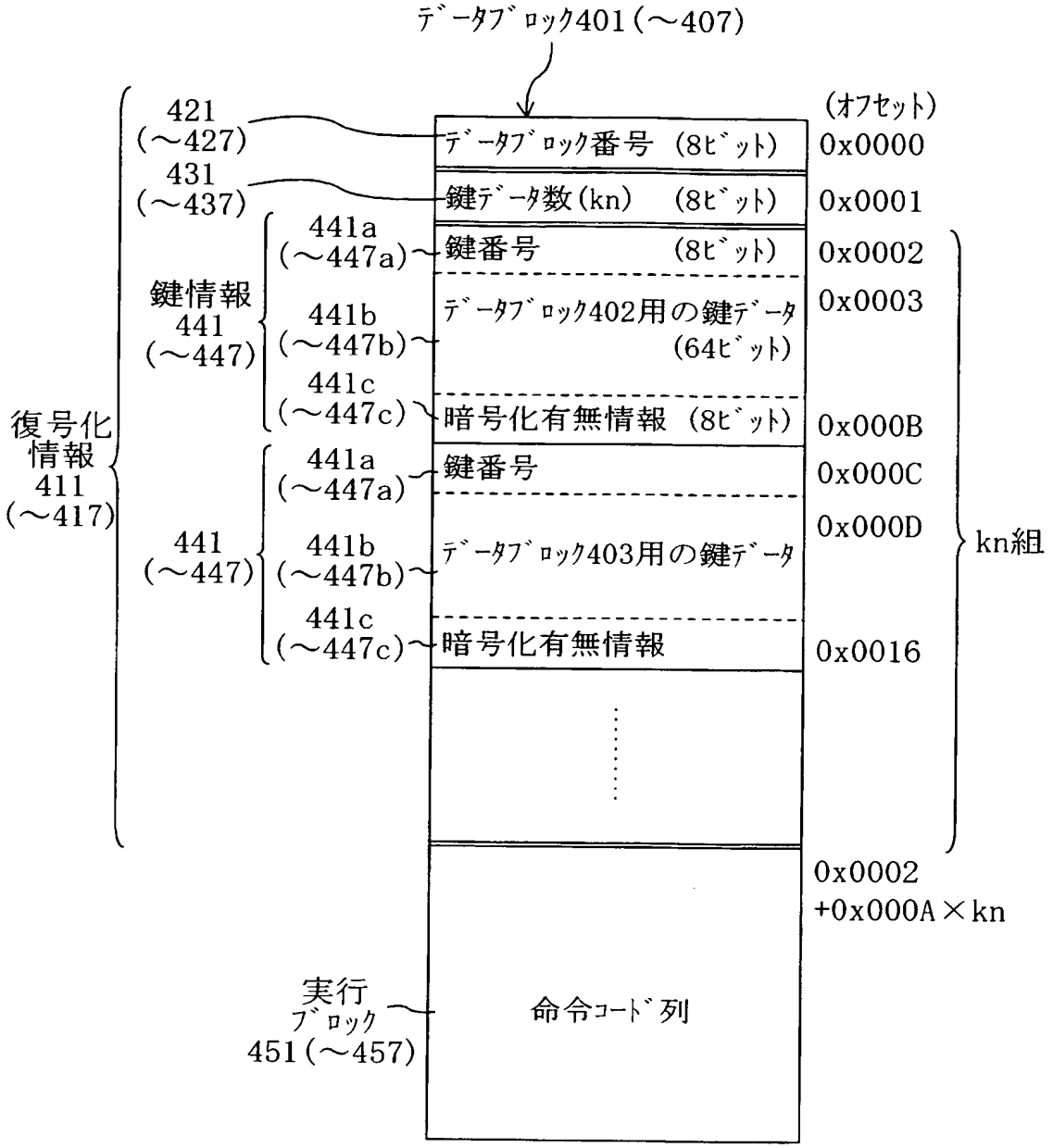

120
メモリ
300
マイクロコンピュータ
102
復号化部
103
鍵データ保持部
304
選択部
105
選択指示保持部
鍵データ
選択指示
306b
306a
306
制御部
鍵テーブル
復号化情報管理部
アドレス
データ(命令コード)
データブロック番号・鍵データ数読み込み信号
鍵情報読み込み信号
データブロック番号
鍵番号、鍵データ、選択指示、
301
CPU
301a
復号化制御部
外部からの初期の鍵番号、鍵データ、選択指示(データブロック401用の鍵番号440a、鍵データ440b、選択指示)

【図７】

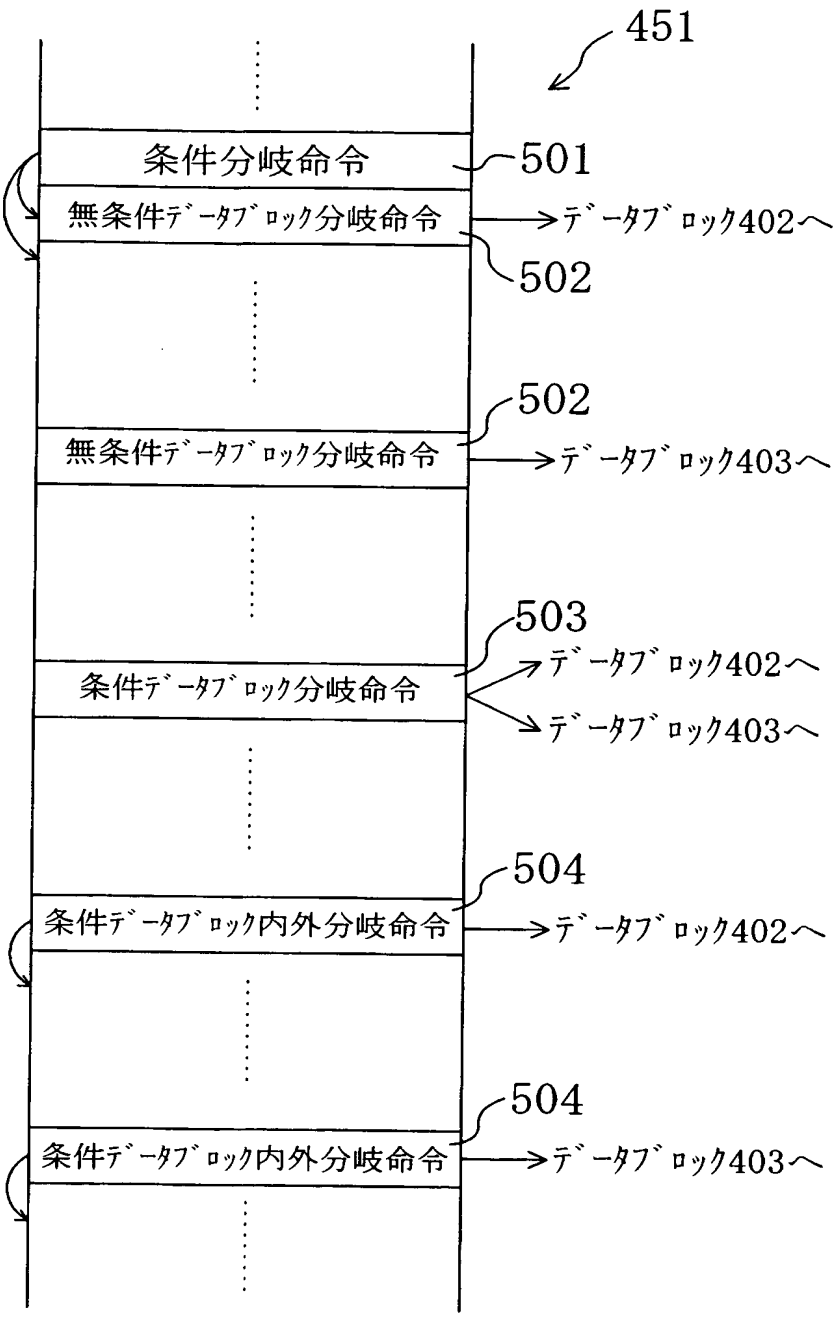
鍵ﾃﾞｰﾌﾞﾙ306aの保持内容

鍵番号	鍵ﾃﾞｰﾀ	選択指示
0x01	0x111111111…	1
0x02	0x222222222…	1
0x03	0x333333333…	0
⋮	⋮	⋮
0x00	0	0
0x00	0	0

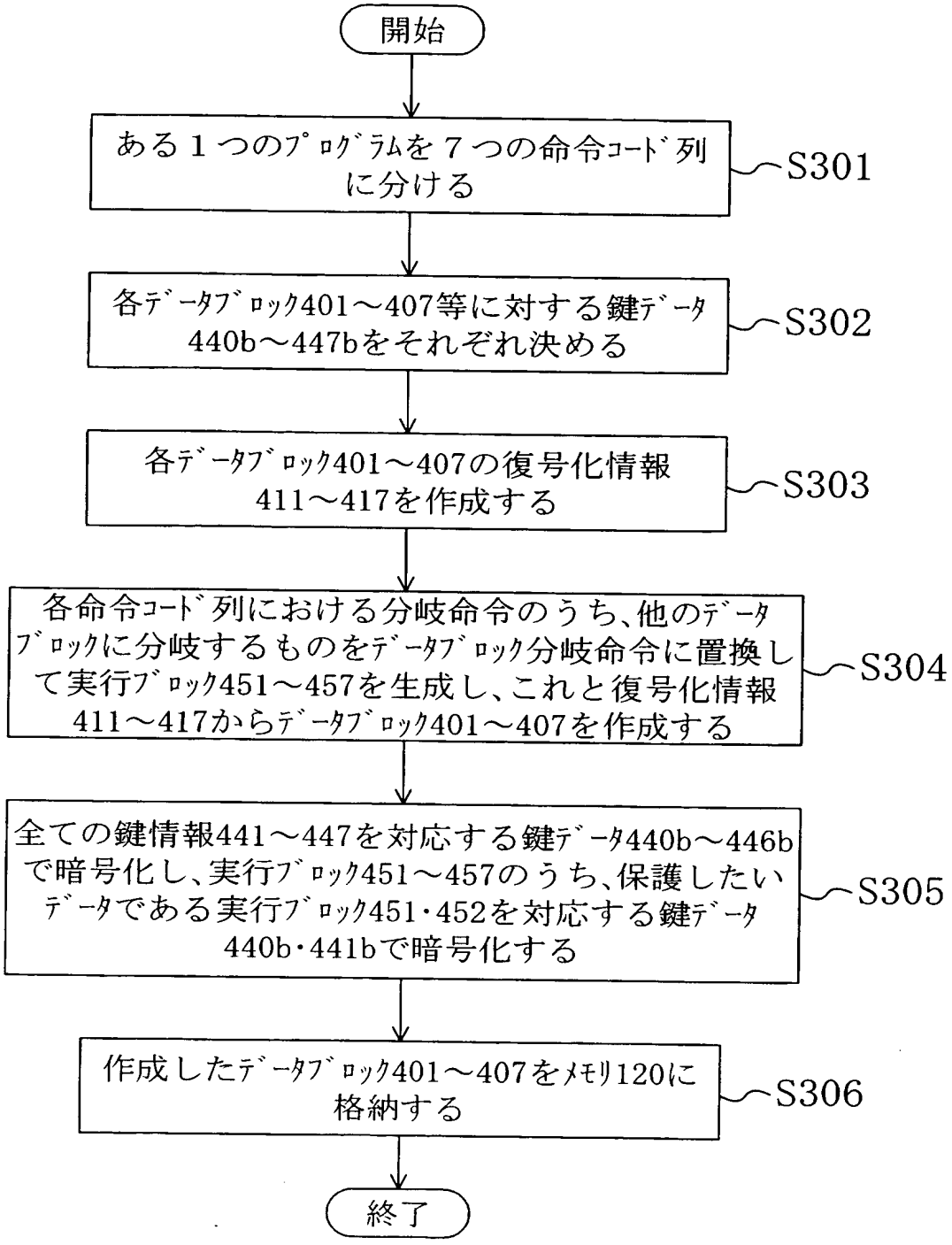
【図８】


データブロック401(～407)
(オフセット)
421
(～427)
データブロック番号 (8ビット)
0x0000
431
(～437)
鍵データ数(kn) (8ビット)
0x0001
441a
(～447a)
鍵番号 (8ビット)
0x0002
鍵情報
441
(～447)
441b
(～447b)
データブロック402用の鍵データ
(64ビット)
0x0003
441c
(～447c)
暗号化有無情報 (8ビット)
0x000B
復号化
情報
411
(～417)
441a
(～447a)
鍵番号
0x000C
441
(～447)
441b
(～447b)
データブロック403用の鍵データ
0x000D
441c
(～447c)
暗号化有無情報
0x0016
kn組
0x0002
+0x000A×kn
実行
ブロック
451(～457)
命令コード列

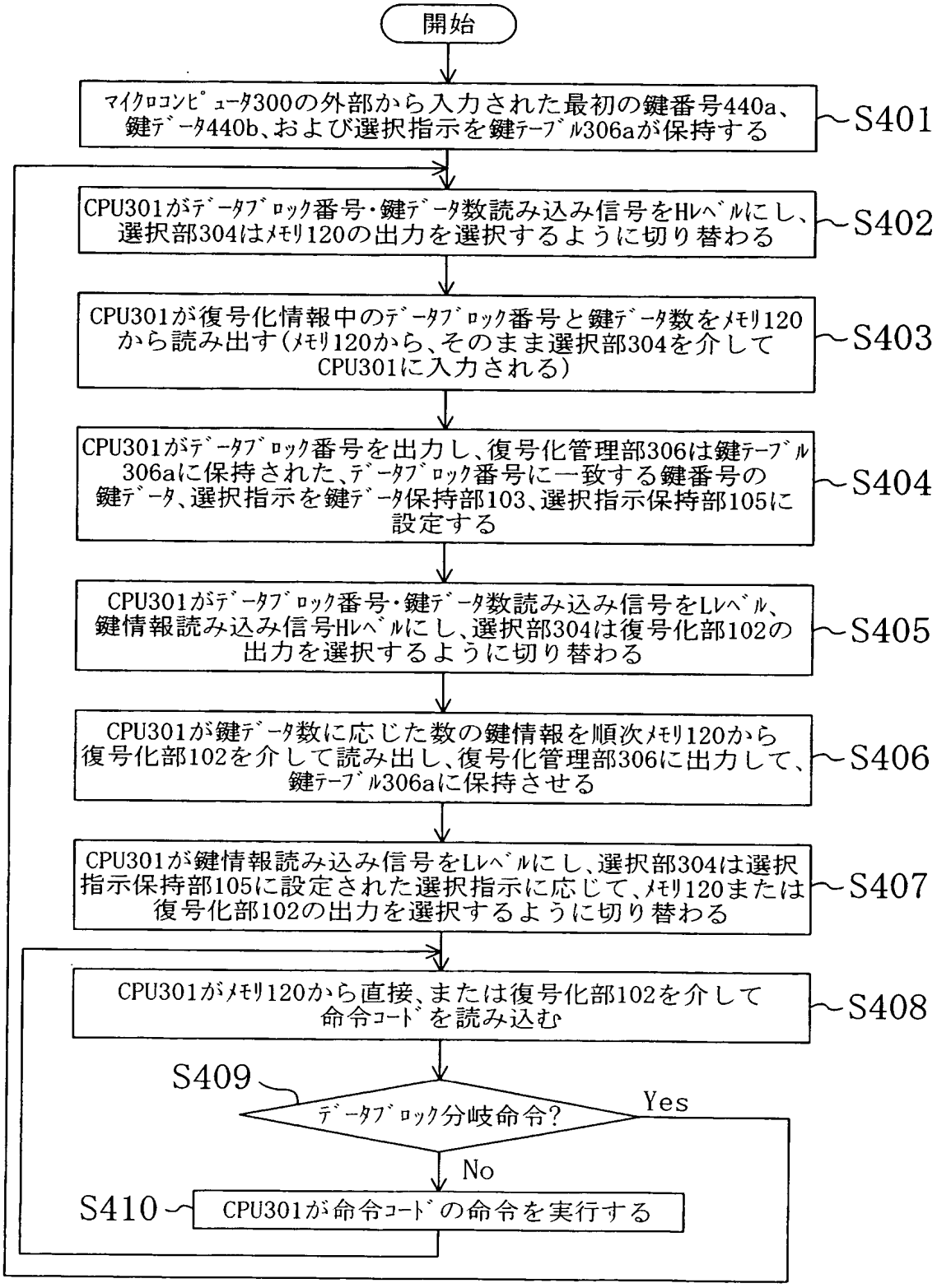
【図９】


451
条件分岐命令
501
無条件ﾃﾞｰﾀﾌﾞﾛｯｸ分岐命令
ﾃﾞｰﾀﾌﾞﾛｯｸ402へ
502
502
無条件ﾃﾞｰﾀﾌﾞﾛｯｸ分岐命令
ﾃﾞｰﾀﾌﾞﾛｯｸ403へ
503
条件ﾃﾞｰﾀﾌﾞﾛｯｸ分岐命令
ﾃﾞｰﾀﾌﾞﾛｯｸ402へ
ﾃﾞｰﾀﾌﾞﾛｯｸ403へ
504
条件ﾃﾞｰﾀﾌﾞﾛｯｸ内外分岐命令
ﾃﾞｰﾀﾌﾞﾛｯｸ402へ
504
条件ﾃﾞｰﾀﾌﾞﾛｯｸ内外分岐命令
ﾃﾞｰﾀﾌﾞﾛｯｸ403へ

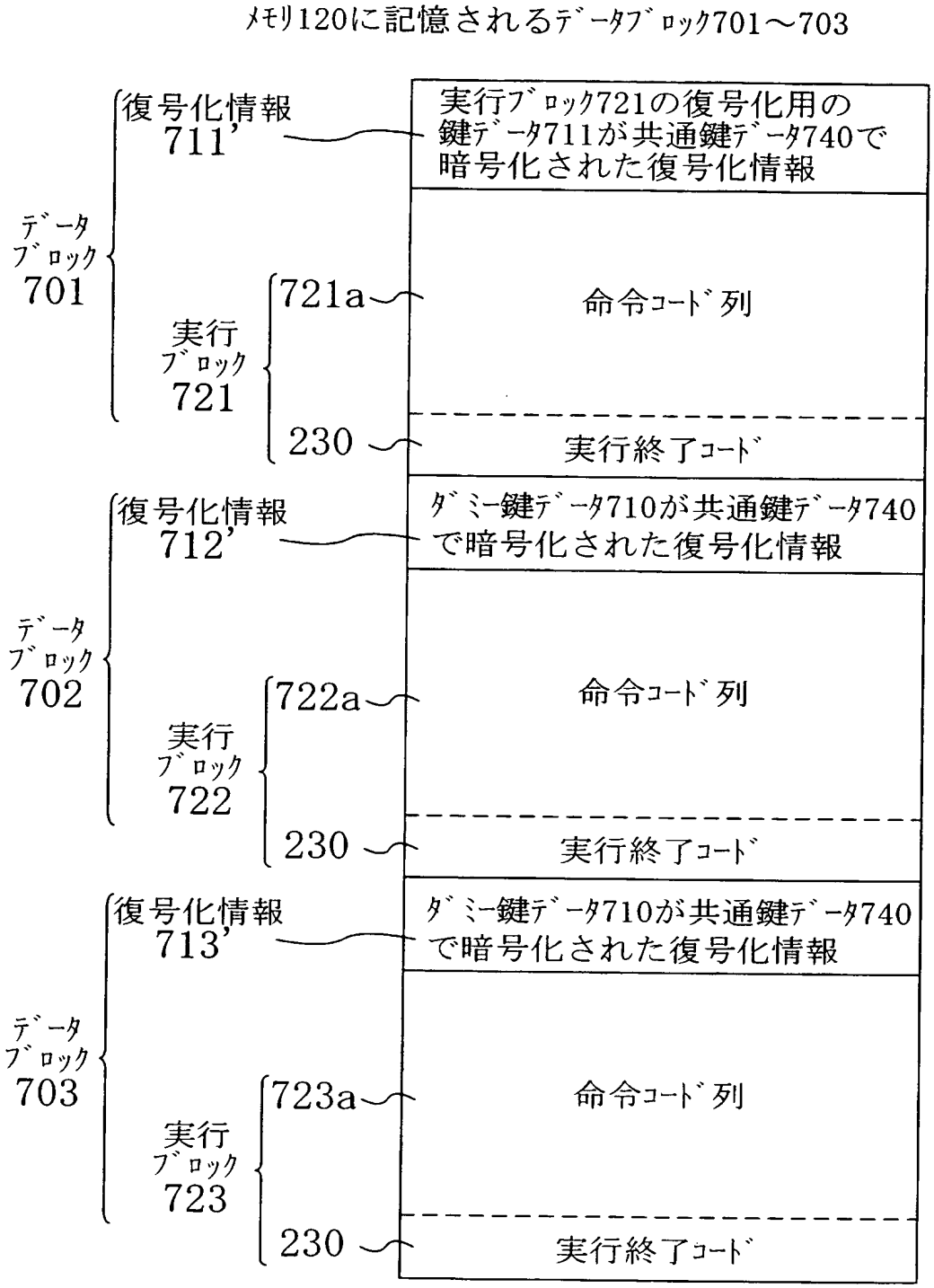
【図１０】


開始
ある１つのﾌﾟﾛｸﾞﾗﾑを７つの命令ｺｰﾄﾞ列に分ける
S301
各ﾃﾞｰﾀﾌﾞﾛｯｸ401～407等に対する鍵ﾃﾞｰﾀ440b～447bをそれぞれ決める
S302
各ﾃﾞｰﾀﾌﾞﾛｯｸ401～407の復号化情報411～417を作成する
S303
各命令ｺｰﾄﾞ列における分岐命令のうち、他のﾃﾞｰﾀﾌﾞﾛｯｸに分岐するものをﾃﾞｰﾀﾌﾞﾛｯｸ分岐命令に置換して実行ﾌﾞﾛｯｸ451～457を生成し、これと復号化情報411～417からﾃﾞｰﾀﾌﾞﾛｯｸ401～407を作成する
S304
全ての鍵情報441～447を対応する鍵ﾃﾞｰﾀ440b～446bで暗号化し、実行ﾌﾞﾛｯｸ451～457のうち、保護したいﾃﾞｰﾀである実行ﾌﾞﾛｯｸ451・452を対応する鍵ﾃﾞｰﾀ440b・441bで暗号化する
S305
作成したﾃﾞｰﾀﾌﾞﾛｯｸ401～407をﾒﾓﾘ120に格納する
S306
終了

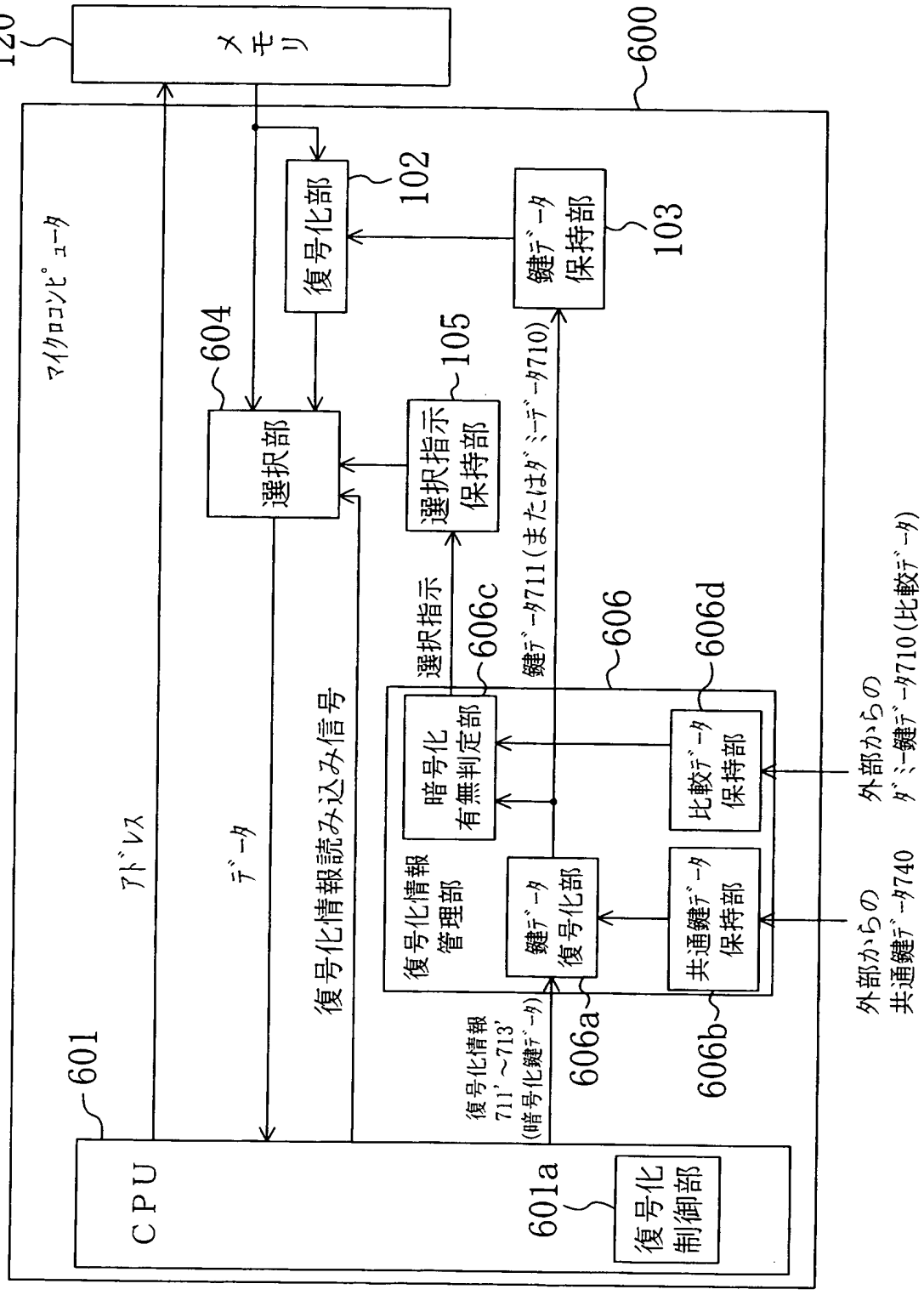
【図１１】


開始
マイクロコンピュータ300の外部から入力された最初の鍵番号440a、鍵データ440b、および選択指示を鍵テーブル306aが保持する
S401
CPU301がデータブロック番号・鍵データ数読み込み信号をHレベルにし、選択部304はメモリ120の出力を選択するように切り替わる
S402
CPU301が復号化情報中のデータブロック番号と鍵データ数をメモリ120から読み出す（メモリ120から、そのまま選択部304を介してCPU301に入力される）
S403
CPU301がデータブロック番号を出力し、復号化管理部306は鍵テーブル306aに保持された、データブロック番号に一致する鍵番号の鍵データ、選択指示を鍵データ保持部103、選択指示保持部105に設定する
S404
CPU301がデータブロック番号・鍵データ数読み込み信号をLレベル、鍵情報読み込み信号Hレベルにし、選択部304は復号化部102の出力を選択するように切り替わる
S405
CPU301が鍵データ数に応じた数の鍵情報を順次メモリ120から復号化部102を介して読み出し、復号化管理部306に出力して、鍵テーブル306aに保持させる
S406
CPU301が鍵情報読み込み信号をLレベルにし、選択部304は選択指示保持部105に設定された選択指示に応じて、メモリ120または復号化部102の出力を選択するように切り替わる
S407
CPU301がメモリ120から直接、または復号化部102を介して命令コードを読み込む
S408
S409
データブロック分岐命令?
Yes
No
S410
CPU301が命令コードの命令を実行する

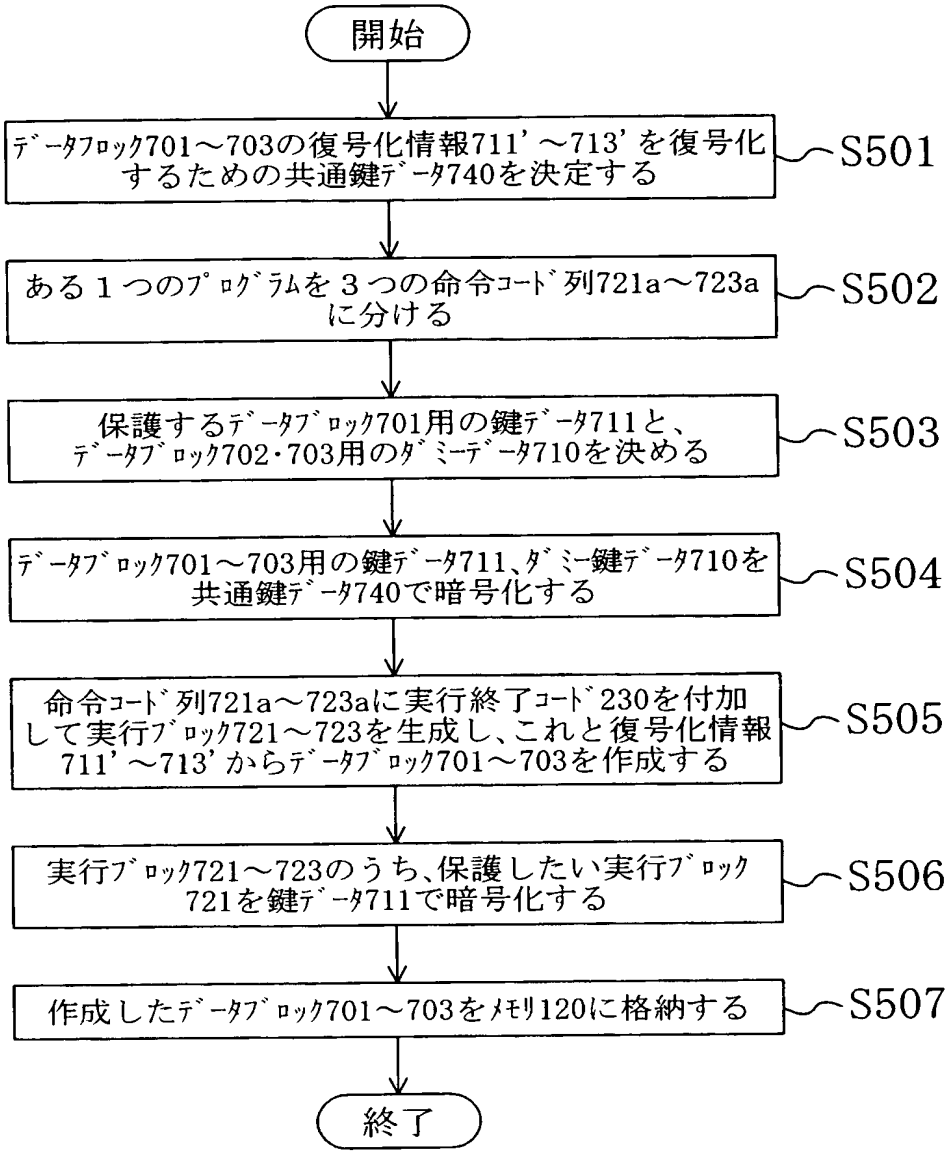
【図１２】


メモリ120に記憶されるデータブロック701～703
復号化情報
711'
実行ブロック721の復号化用の
鍵データ711が共通鍵データ740で
暗号化された復号化情報
データ
ブロック
701
721a
命令コードド列
実行
ブロック
721
230
実行終了コード
復号化情報
712'
ダミー鍵データ710が共通鍵データ740
で暗号化された復号化情報
データ
ブロック
702
722a
命令コードド列
実行
ブロック
722
230
実行終了コード
復号化情報
713'
ダミー鍵データ710が共通鍵データ740
で暗号化された復号化情報
データ
ブロック
703
723a
命令コードド列
実行
ブロック
723
230
実行終了コード

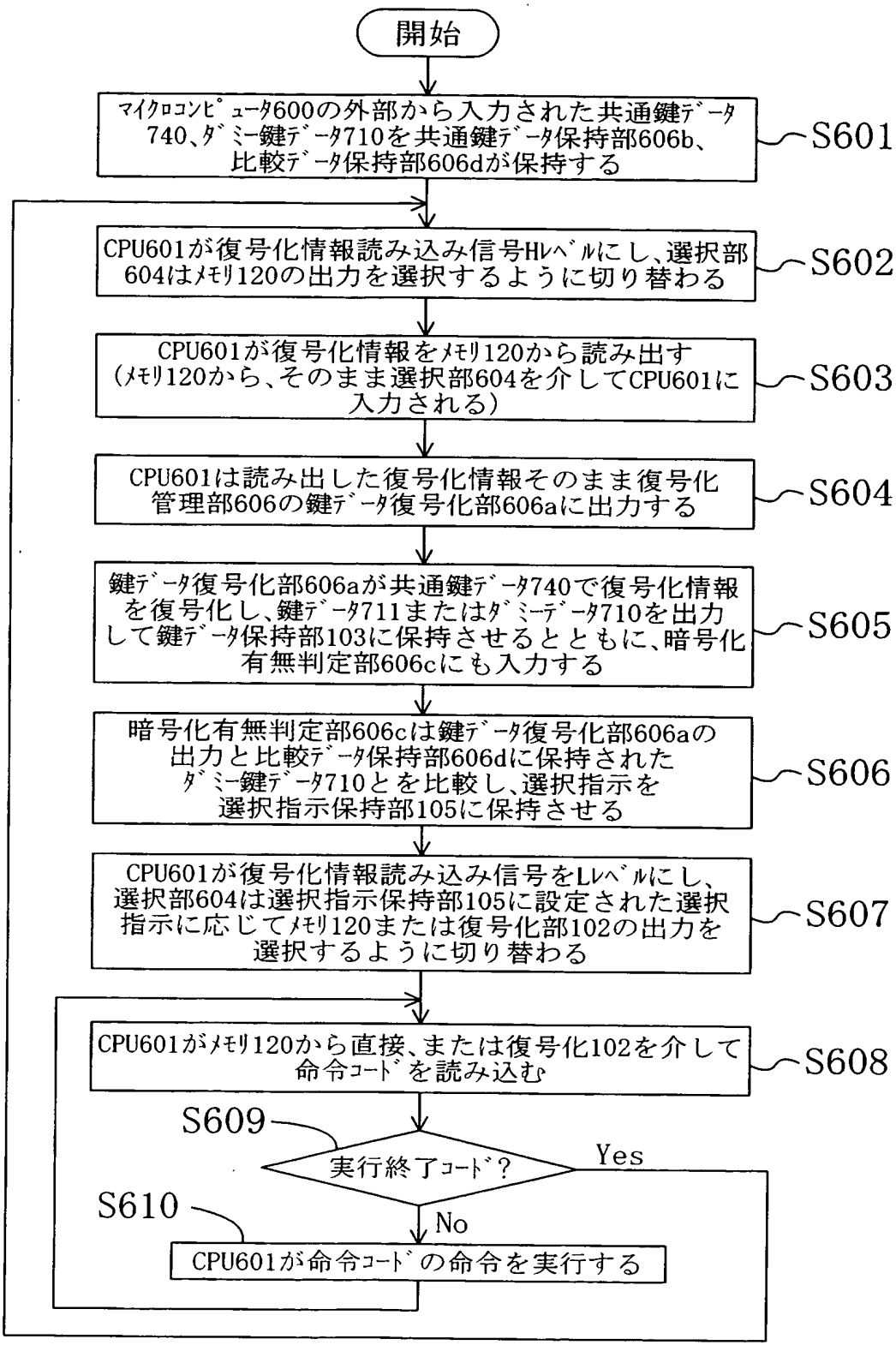
【図１３】


120
メモリ
600
マイクロコンピュータ
102
復号化部
103
鍵データ保持部
604
選択部
105
選択指示保持部
選択指示
606c
606
606d
鍵データ711（またはダミーデータ710）
暗号化有無判定部
比較データ保持部
復号化情報管理部
鍵データ復号化部
共通鍵データ保持部
アドレス
データ
復号化情報読み込み信号
外部からのダミー鍵データ710（比較データ）
外部からの共通鍵データ740
復号化情報711'～713'（暗号化鍵データ）
601
606a
606b
CPU
601a
復号化制御部

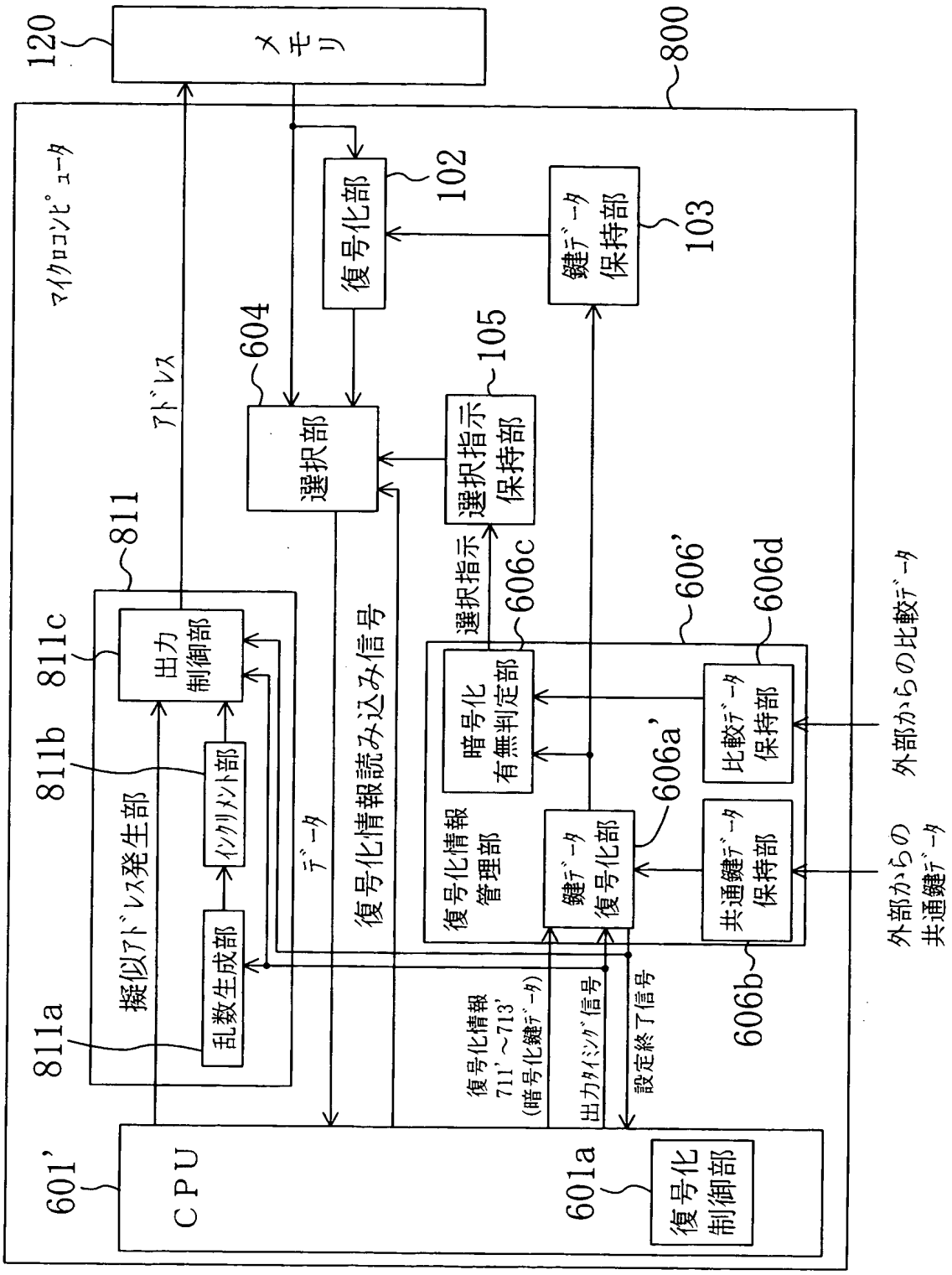
【図１４】


開始
ﾃﾞｰﾀﾌﾛｯｸ701～703の復号化情報711'～713'を復号化するための共通鍵ﾃﾞｰﾀ740を決定する
S501
ある１つのﾌﾟﾛｸﾞﾗﾑを３つの命令ｺｰﾄﾞ列721a～723aに分ける
S502
保護するﾃﾞｰﾀﾌﾞﾛｯｸ701用の鍵ﾃﾞｰﾀ711と、ﾃﾞｰﾀﾌﾞﾛｯｸ702・703用のﾀﾞﾐｰﾃﾞｰﾀ710を決める
S503
ﾃﾞｰﾀﾌﾞﾛｯｸ701～703用の鍵ﾃﾞｰﾀ711、ﾀﾞﾐｰ鍵ﾃﾞｰﾀ710を共通鍵ﾃﾞｰﾀ740で暗号化する
S504
命令ｺｰﾄﾞ列721a～723aに実行終了ｺｰﾄﾞ230を付加して実行ﾌﾞﾛｯｸ721～723を生成し、これと復号化情報711'～713'からﾃﾞｰﾀﾌﾞﾛｯｸ701～703を作成する
S505
実行ﾌﾞﾛｯｸ721～723のうち、保護したい実行ﾌﾞﾛｯｸ721を鍵ﾃﾞｰﾀ711で暗号化する
S506
作成したﾃﾞｰﾀﾌﾞﾛｯｸ701～703をﾒﾓﾘ120に格納する
S507
終了

【図１５】


開始
ﾏｲｸﾛｺﾝﾋﾟｭｰﾀ600の外部から入力された共通鍵ﾃﾞｰﾀ740、ﾀﾞﾐｰ鍵ﾃﾞｰﾀ710を共通鍵ﾃﾞｰﾀ保持部606b、比較ﾃﾞｰﾀ保持部606dが保持する
S601
CPU601が復号化情報読み込み信号Hﾚﾍﾞﾙにし、選択部604はﾒﾓﾘ120の出力を選択するように切り替わる
S602
CPU601が復号化情報をﾒﾓﾘ120から読み出す（ﾒﾓﾘ120から、そのまま選択部604を介してCPU601に入力される）
S603
CPU601は読み出した復号化情報そのまま復号化管理部606の鍵ﾃﾞｰﾀ復号化部606aに出力する
S604
鍵ﾃﾞｰﾀ復号化部606aが共通鍵ﾃﾞｰﾀ740で復号化情報を復号化し、鍵ﾃﾞｰﾀ711またはﾀﾞﾐｰﾃﾞｰﾀ710を出力して鍵ﾃﾞｰﾀ保持部103に保持させるとともに、暗号化有無判定部606cにも入力する
S605
暗号化有無判定部606cは鍵ﾃﾞｰﾀ復号化部606aの出力と比較ﾃﾞｰﾀ保持部606dに保持されたﾀﾞﾐｰ鍵ﾃﾞｰﾀ710とを比較し、選択指示を選択指示保持部105に保持させる
S606
CPU601が復号化情報読み込み信号をLﾚﾍﾞﾙにし、選択部604は選択指示保持部105に設定された選択指示に応じてﾒﾓﾘ120または復号化部102の出力を選択するように切り替わる
S607
CPU601がﾒﾓﾘ120から直接、または復号化102を介して命令ｺｰﾄﾞを読み込む
S608
S609
実行終了ｺｰﾄﾞ？
Yes
No
S610
CPU601が命令ｺｰﾄﾞの命令を実行する

【図１６】


120
メモリ
800
マイクロコンピュータ
102
復号化部
103
鍵データ保持部
604
選択部
105
選択指示保持部
811
811c
出力制御部
811b
インクリメント部
811a
擬似アドレス発生部
乱数生成部
アドレス
データ
復号化情報読み込み信号
選択指示
606c
606'
606d
暗号化有無判定部
復号化情報管理部
606a'
鍵データ復号化部
比較データ保持部
共通鍵データ保持部
606b
復号化情報711'～713'(暗号化鍵データ)
出力タイミング信号
設定終了信号
601'
CPU
601a
復号化制御部
外部からの比較データ
外部からの共通鍵データ

【書類名】　要約書

【要約】

【課題】　復号化鍵の管理を複雑化することなく、記憶データの秘匿性を高める。

【解決手段】　メモリ１２０に記憶される各データブロックは、元のプログラムが分割されて、それぞれ異なる鍵データで暗号化された実行ブロックと、次に読み込まれるデータブロックを復号化するための暗号化された鍵データを含む復号化情報とを含んでいる。上記データブロックがマイクロコンピュータ１００に読み込まれると、復号化部１０２により復号化された復号化情報中の鍵データは鍵データ一時保持部１０６ａに保持された後、次のデータブロックが読み込まれる際に鍵データ保持部１０３に保持される。そこで、上記復号化され保持された鍵データによって、次のデータブロックの復号化情報および実行ブロックが復号化される。

【選択図】　図１

特願２００３－０５５６２６

出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社